Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Gouverner la technologie en temps de crise

Poullet, Yves

Publication date:
2020

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2020, *Gouverner la technologie en temps de crise: aide à la décision dans le cadre du Covid-19*. s.n., s.l.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

HUMAN TECHNOLOGY
FOUNDATION

GOUVERNER LA TECHNOLOGIE EN TEMPS DE CRISE

AIDE À LA DÉCISION DANS LE CADRE DU COVID-19

SOMMAIRE

Le présent rapport ne constitue pas un avis juridique et n'est communiqué qu'à titre informationnel.

AVANT-PROPOS

L'épidémie est, dans l'imaginaire collectif, l'un des fléaux qui menacent notre espèce. La crise du COVID-19 aura montré qu'elle peut aussi, de façon concrète et violente, désorganiser notre société et paralyser l'économie mondiale. Face à cette situation qui sollicite les décideurs politiques et les dirigeants d'entreprise, le recours à la technologie est assurément d'une aide précieuse, tant pour lutter contre la pandémie que pour réorganiser l'activité à moyen terme. La place prise par les dispositifs technologiques pose également des questions d'ordre éthique.

Fidèle à sa mission, la Human Technology Foundation, sollicitée par ses partenaires, a entrepris la présente étude afin de déterminer comment, dans le contexte actuel, l'usage de la technologie peut toujours se faire au bénéfice de l'humain. Cette étude a été dirigée par un comité de pilotage dont la présidence a été confiée à Jean-Louis Davet, président de Denos Health Management.

Le travail a été mené selon la méthode propre à notre fondation, de façon internationale et pluridisciplinaire, croisant les regards de spécialistes des technologies étudiées, de juristes et d'éthiciens, et en nous appuyant sur les équipes de nos bureaux de Paris et Montréal.

Nous avons collaboré avec des chercheurs de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) et des enseignants-chercheurs de plusieurs universités situées à Montréal, Lille, Sherbrooke et Namur. Y ont aussi pris part des avocats membres du réseau ITechLaw et des collaborateurs d'entreprises partenaires, comme Samsung et EY. L'étude a aussi été soutenue par des institutions comme la Chambre de la sécurité financière du Québec et la Mutualité Française.

Je tiens à remercier la trentaine d'experts qui se sont ainsi mobilisés pour apporter leurs compétences, et particulièrement les membres du comité de pilotage et de l'équipe de coordination.

Au-delà de cette crise, nous espérons que la méthode développée et exposée dans le présent rapport sera utile pour sélectionner et gouverner des dispositifs technologiques dans ce contexte nouveau, probablement appelé à durer.

Bonne lecture.

Eric Salobir
Président du comité exécutif
Human Technology Foundation

INTRODUCTION

JAMAIS PANDÉMIE NE S'EST PROPAGÉE DANS UN MONDE AUSSI RICHE DE TECHNOLOGIES ET DE DONNÉES. FAUTE D'AVOIR PERMIS À TOUS LES PAYS DE SUFFISAMMENT ANTICIPER L'IMPACT DU COVID-19 DÈS SON ÉMERGENCE, **LA PUISSANCE DU NUMÉRIQUE S'EST PARTOUT MOBILISÉE** POUR ACCÉLÉRER LA RECHERCHE SCIENTIFIQUE, LIMITER L'EXPANSION DE L'ÉPIDÉMIE ET AUJOURD'HUI FACILITER LA REPRISE DE L'ACTIVITÉ ÉCONOMIQUE.

Mais le recours à cet atout considérable peut lui aussi présenter ses propres risques et provoquer l'inquiétude jusqu'à freiner l'adoption des solutions proposées. Souvent pris dans un faisceau de contraintes, voire d'injonctions contradictoires, les décideurs publics et privés se retrouvent ainsi devant des arbitrages cornéliens. S'entrechoquent notamment les **enjeux d'efficacité sanitaire**, de **préservation de libertés individuelles**, de **souveraineté numérique**, **d'inclusion sociale** et **d'adoption large** des dispositifs proposés.

Le citoyen interpelle le politique sur la portée sociale des dispositifs technologiques et sanitaires qu'il envisage. L'entreprise sollicite les autorités, en attente de préconisations concrètes à suivre et d'un cadre circonscrivant ses responsabilités. L'employé interpelle son employeur sur la réalité de ses engagements socialement responsables et la sécurité qu'il lui doit au travail. L'État se retourne vers divers corps intermédiaires susceptibles de faciliter l'adoption des dispositifs dont il recommande l'utilisation sans pour autant les imposer. Et l'entreprise est amenée elle aussi à peser les moyens et relais dont elle dispose pour promouvoir l'adoption des solutions de protection auprès de ses employés. Le client s'interroge sur le bien-fondé d'être contraint par le propriétaire d'un commerce à utiliser tel ou tel dispositif pour entrer dans le magasin, voire pour bénéficier de conditions privilégiées. Autant de situations différentes. Autant de postures et de valeurs éthiques invoquées par les uns et les autres, à charge ou à décharge. Et au final, autant de **dilemmes** et de **tensions pour celui qui décide ou orchestre** la mise en œuvre de dispositifs technologiques de protection sanitaire.

C'est à ces décideurs que le présent rapport et la méthode qu'il propose s'adressent prioritairement. La démarche vise à leur fournir des clés d'analyse et d'arbitrage dans l'emploi des technologies pour sécuriser la sortie de crise et accélérer un retour sain à l'activité. **Deux niveaux de lecture** sont proposés : un premier niveau s'adressant aux décideurs de tout type d'organisations et d'instances de gouvernance, et un second niveau plus spécifique aux entreprises.

Développée dans le contexte du COVID-19, la méthode présentée préfigure en fait une approche plus générale (qui fera l'objet de prochains travaux) pour la mise en œuvre de dispositifs algorithmiques et de traitement de données personnelles dont l'adoption et la bonne utilisation appellent des considérations éthiques fondamentales.

Cette approche se décline assez naturellement à **d'autres domaines liés à la santé**, dans lesquels la crise a catalysé des tendances de fond déjà amorcées, traçant la voie vers des services de santé de plus en plus numérisés et consommateurs de données. Plus largement encore, cette méthode pourra être adaptée pour **faire de l'éthique non pas une contrainte mais un « *enabler* »** pour le développement de services numériques dont le caractère sensible nécessite une approche circonstanciée au sein de nos sociétés démocratiques.

L'approche méthodologique que nous proposons est structurée par étapes :

- La constitution d'un **organe de gouvernance** approprié, qui regroupe l'ensemble des parties prenantes et qui pilote le projet depuis sa conception jusqu'à son arrêt (retour à des conditions sanitaires « normales »), doté de compétences techniques, éthiques et juridiques.

- La construction d'un **cadre de référence commun**. Les analogies avec des situations connues (peste, guerre, terrorisme, surveillance de masse, etc.), souvent employées, interpellent notre imaginaire et structurent notre compréhension de la situation.

De tels biais prédéterminent tant les solutions choisies par les décideurs que les rejets et oppositions de ceux à qui elles s'adressent. Le choix du référentiel est donc clé. Il permet en outre de fédérer une vision commune des enjeux.

- La **qualification précise du besoin** (traçage des individus porteurs du virus, étude des comportements à l'échelle collective, contrôle du respect des mesures sanitaires, contrôle de l'accès à des espaces privés, etc.), en considérant bien la **globalité du dispositif sanitaire** dans lequel les solutions technologiques s'insèrent.

- L'analyse approfondie des **technologies disponibles** et des enjeux (techniques, sécuritaires, éthiques, juridiques,, etc.) liés à leur déploiement.

- Sur les bases précédentes, le déroulement d'un **processus de décision s'appuyant sur une grille multifactorielle**, dont l'emploi doit associer tous les acteurs du projet. Les considérations abordées à cette occasion permettent par ailleurs de cerner les risques et la manière de les atténuer, de préparer les conditions d'une adoption large des dispositifs retenus, et d'en fixer les conditions de gouvernance et d'évolution dans le temps.

Ce rapport est ainsi constitué de trois grandes parties.

- La première se concentre sur les **dimensions anthropologiques, sociales et éthiques liées aux enjeux et aux moyens technologiques de sortie de crise sanitaire**. Y sont notamment discutés les différents référentiels, principes et valeurs susceptibles de conduire à l'indispensable **cadre de référence commun** précédemment évoqué. Les lecteurs désireux d'approfondir davantage cet aspect de la situation sont invités à consulter l'**annexe n° 1** où l'argumentation est davantage développée.

- La deuxième partie dresse un **panorama des principales technologies disponibles** au regard des enjeux sanitaires, techniques et sociétaux. Une attention toute particulière est portée aux questions les plus structurantes, comme par exemple la nature des données collectées, les modalités de traitement et de stockage de ces données (centralisées/décentralisées/hybrides), les aspects sécuritaires liés à la technologie utilisée, etc. Cette partie a également pour ambition de **rendre la dimension technologique accessible aux décideurs** non issus de cette branche d'activité.

- La troisième partie expose en détail **la méthodologie et les outils** qui l'accompagnent. La grille d'analyse d'impact multifactorielle que nous avons développée et son mode d'emploi y sont présentés, l'intégralité de cet outil figurant en annexe. **La méthode a été intégralement appliquée à une sélection de dispositifs illustrant la diversité des solutions technologiques anti-COVID-19 développées à travers le monde.** Très pratiquement, onze solutions ont ainsi fait l'objet d'une analyse approfondie, menée par une équipe internationale constituée d'experts de la technologie, de la santé, d'éthiciens et de juristes. **Les résultats et enseignements de ces travaux illustrent les différentes rubriques du rapport et guident nos recommandations.** Des annexes présentent un tableau comparatif de ces onze dispositifs, ainsi que les résumés des analyses menées sur chacun d'entre eux.

Jean-Louis Davet
Président de DENOS Health Management
Senior Advisor Human Technology Foundation

CHAPITRE 1

CONTEXTE ET MISE EN PERSPECTIVE

Tout **décideur**, public comme privé, institution comme entreprise, se retrouve aujourd'hui confronté à un déferlement de positions mettant en avant des arguments d'ordre éthique face aux solutions technologiques de sortie de crise sanitaire qu'il envisage. Mais, au regard de la complexité d'une situation de pandémie, la satisfaction de chacun des arguments puisant sa légitimité dans l'éthique conduirait à paralyser toute action. **Une clarification des principes juridico-éthiques à privilégier est donc inévitable.**

L'acceptabilité sociale du recours à une technologie ne repose pas seulement sur le fait que celle-ci soit accessible, efficace, explicable et aisément employable pour un large public, ni sur les précautions techniques, juridiques et éthiques qui l'accompagnent. Notre degré d'acceptabilité dépend aussi des référentiels que nous sollicitons pour comprendre l'inconnu à partir du connu. Or, cette crise a provoqué un véritable **conflit des référentiels**. Tout décideur doit déterminer le registre de signification à solliciter face à la situation actuelle, pour faciliter l'adoption de l'outil choisi et sa contribution à la réalisation d'un futur souhaitable.

Chaque référentiel peut introduire, dans l'approche des mesures à mettre en oeuvre, des **biais** qui lui sont propres. Ces biais influencent tant les décideurs que ceux à qui ils s'adressent. Ils prédéterminent des solutions spécifiques pour les uns, et des rejets et des oppositions pour les autres.

Le référentiel de **précédentes grandes épidémies**, comme la peste, le choléra ou le sida, interpellent fortement notre imaginaire, conduisant à surrréagir ou au contraire à minimiser la gravité du COVID-19. Le référentiel de la **surveillance** de masse pousse à considérer le déploiement de dispositifs technologiques comme inconciliable avec la préservation des libertés individuelles. D'autres référentiels plus éclairants devraient au contraire être mobilisés. C'est le cas du référentiel de notre **relation avec la nature** qui nous invite à prendre collectivement conscience de notre responsabilité partagée dans la crise actuelle. Plus particulièrement, **le référentiel du soin** implique de fonder les stratégies de sortie de crise sur des principes de gouvernance inclusive, de dialogue, de solidarité et d'équité, de responsabilisation et de confiance. Il paraît ainsi le plus constructif. Il évite notamment les écueils d'autres référentiels comme ceux de la **guerre** et du **terrorisme**, qui induisent d'une part, que la responsabilité de nous défendre incombe à l'État et d'autre part, que le danger nous est extérieur, alors que nous pouvons tous être porteurs du virus et sommes donc tous en partie responsables de la solution.

Nous sommes tous en danger face à autrui et en même temps un danger pour autrui. **Le référentiel du soin appelle ainsi à la recherche incessante d'un juste compromis entre le besoin de liberté de choix des individus et la responsabilité de chacun pour autrui, tout en accordant une attention particulière à la protection des populations les plus vulnérables.**

UN RAPPORT AMBIVALENT AUX TECHNOLOGIES

Face à l'urgence de la situation, une multitude de projets numériques se développe aujourd'hui à travers le monde pour tenter de trouver des moyens d'adresser les problèmes posés par le SARS-COV-2 (COVID-19). L'enjeu commun de ces dispositifs technologiques est de tracer la transmission et la propagation du virus dans la population, tant au niveau local, régional, national, qu'international, afin de contenir sa contagion, de permettre un retour à la vie normale et d'éviter un rebond épidémique.

Ces développements sont porteurs d'espoir, car le recours à des technologies médicales et des outils de santé publique innovants pourraient apporter des moyens de lutte efficaces contre les microbes. Mais un recours aux innovations numériques actuelles n'est pas non plus sans risques et soulève d'importantes questions de société. Leur mésusage et l'extension de leurs objets à d'autres finalités que leur buts initiaux - que ce soit par les pouvoirs publics ou des acteurs privés (usage policier menant à des contrôles excessifs, contrôle par l'employeur, utilisation par les assureurs, etc.) - nécessitent de garantir que la collecte et le traitement des données respectent des cadres éthiques et juridiques clairs et protecteurs des droits et libertés individuelles des personnes. A défaut de quoi, ils peuvent affecter profondément la confiance de la population dans les porteurs de ces projets, et donc nuire à la coopération sociale que requiert une lutte contre une pandémie.

L'ambivalence du rapport des humains aux technologies soulève donc des **questions pratiques** d'ordre aussi bien **épistémologique** (Que pouvons-nous connaître grâce à la technologie ? Cette information est-elle fiable ?), **éthique et juridique** (Sous quelles conditions pouvons-nous prétendre à certains biens en utilisant une technologie ? Quelles règles doivent encadrer son usage ? Quels sont les risques et sont-ils répartis de façon équitable ?) que **politique** (Comment gouvernons-nous le déploiement et l'usage d'une technologie dans une société donnée ?).

UNE ÉTHIQUE PRATIQUE POUR GUIDER LA PRISE DE DÉCISIONS

Dans des circonstances marquées par la crainte, l'incertitude, et parfois la défiance, chaque décideur se retrouve aujourd'hui confronté à un déferlement de positions mettant en avant des arguments d'ordre éthique face aux solutions qu'il envisage : que ce soit les **gouvernements**, quant aux dispositifs nationaux ; les **employeurs**, quant aux solutions qu'ils pourraient mettre en place pour protéger leurs **salariés** ; les commerces et transports, pour leurs **clients** ; les **propriétaires** immobiliers pour leurs **locataires** ; etc.

D'un tel contexte émergent des enjeux qui pourraient conduire à l'exclusion de toutes les solutions proposées et donc à la paralysie. Par ailleurs, la polarisation du débat sur certains aspects les plus médiatisés de la lutte contre le COVID-19 rend difficile la prise en compte de la situation dans son intégralité. Par exemple, si les arguments avancés par les défenseurs des libertés individuelles et de la vie privée sont indéniablement pertinents et essentiels, la dimension de « privacy by design » n'épuise pas, à elle seule, les questions éthiques posées par la mise en œuvre de solutions techniques. Dès lors, il s'agit de trouver un **juste équilibre** entre l'objectif de **santé publique (le droit à la santé)** et les diverses **libertés** entravées par le confinement, que ce soient des libertés de **mouvement**, de **réunion** et **d'expression**, de la **vie privée** mais également de **l'équité** ou de **la non-discrimination**, également garanties aux citoyens et qui pourraient être compromises par certaines utilisations des données. Notamment, si certaines applications peuvent faciliter la recherche des contacts par les acteurs de santé publique ou les employeurs, elles peuvent également conduire à la stigmatisation ou à l'exclusion sociale de populations déjà vulnérables, renforçant ainsi des injustices et des inégalités préexistantes. A titre d'illustration, la question de l'accès à ces dispositifs numériques - que ce soit en termes de coûts, d'équité, ou d'acceptabilité sociale - se pose plus que jamais avec insistance. Si en France 80 % des citoyens sont équipés de smartphones, son taux de pénétration n'est que de 30 % en Inde, sans évoquer la distribution disparate au sein même de la population, en fonction notamment des catégories d'âges ou des milieux sociaux. En d'autres termes, ces populations ne peuvent bénéficier de façon équitable des solutions de traçage automatique fondées sur la possession d'un smartphone.

Ainsi, c'est à l'aune d'une **conception plus large de l'éthique** que les différents dispositifs envisagés doivent être expliqués à des citoyens (en tant qu'**individus** mais aussi en tant que **groupes** ou

communautés) et arbitrés par eux. Les citoyens ne peuvent être réduits au statut de simples **utilisateurs** d'outils numériques: ils sont coresponsables des solutions à mettre en oeuvre puisqu'ils participent tous à la création du risque. Une éthique pratique donc, non pas brandie comme l'affirmation d'une morale particulière, mais conçue comme une démarche réflexive, ouverte et concrète appuyée sur une véritable discussion des valeurs et priorités souhaitées pour notre société, pour évaluer, choisir et gouverner les solutions technologiques en sortie de crise sanitaire.

PASSER D'UNE GESTION DE CATASTROPHE À UNE GESTION DES RISQUES SUR LE LONG TERME

L'âpreté des débats quant aux solutions technologiques développées dans l'urgence de la crise sanitaire actuelle révèle le véritable défi de gouvernance (pour les acteurs étatiques, pour l'industrie, pour toute organisation et pour la société civile), dans la durée, qui se présente à nous.

D'une part, l'incertitude demeure aujourd'hui importante à de nombreux titres, concernant notamment des interrogations sur les possibles mutations du virus, la réalité et la durée de l'immunité acquise, la saisonnalité et la possibilité de rebonds épidémiques. Même lorsqu'un **vaccin** sera disponible et, espérons-le, largement accessible de façon équitable à toute la population de la planète, nous serons confrontés demain à de **nouvelles épidémies** qui pourraient tout autant nous surprendre. D'autre part, notre capacité à mobiliser la puissance des technologies et du numérique pour prévenir ou protéger les populations est un atout nouveau et majeur de nos sociétés face aux fléaux sanitaires. Mais les modalités pour recourir à ces dispositifs porteront, elles aussi, leur part de risque sur le long terme, notamment en matière de souveraineté (régionale, nationale et internationale) ou de protection des intérêts et des libertés des utilisateurs. C'est bien dans ce contexte d'exposition permanente à de tels risques que nous devons apprendre à gouverner l'élaboration et la mise en oeuvre de solutions.

Ainsi, les processus tant d'association des parties prenantes, d'analyse et d'arbitrage entre dispositifs que de facilitation de l'acceptabilité éthique et d'acceptation sociale qui seront développés pour juguler le COVID-19 pourront constituer une première ébauche du mode de gouvernance d'un

avenir où tant les technologies et l'algorithmique que les risques extrêmes, sanitaires ou non, seront prégnants et nous conduiront à peser nos décisions au regard de considérations éthiques globales.

L'ACCEPTABILITÉ SOCIALE D'UNE TECHNOLOGIE

La question de ***l'accès*** aux technologies et de leur ***acceptabilité sociale*** est largement soulignée dans le contexte des débats actuels sur les technologies de traçage numérique. Ces technologies (applications, montres, bracelets connectés, etc.) pourraient accompagner et faciliter la reprise des activités sociales, économiques et culturelles. Parmi les conditions d'efficacité de telles technologies, les études sont encore très peu nombreuses. L'une d'entre elles - largement reprises depuis - souligne la nécessité qu'une proportion suffisante de la population (environ 60 %, cf. *Big Data Institute, Nuffield Department of Medicine, Oxford University* dirigé par le Dr. Christophe Fraser) en fasse usage, sans quoi leur couverture des mouvements individuels ou collectifs serait inefficace pour suivre la transmission d'un virus à l'échelle d'un territoire. En raison du taux élevé d'usage volontaire auquel est donc conditionnée l'efficacité de ces technologies, plusieurs pays privilégient à ce jour des **solutions de traçage alternatives plus classiques** qui ont fait leur preuve en santé publique (centres d'appels téléphoniques, traçage par le personnel de santé). Le problème de cette approche est qu'elle demande beaucoup de personnel et énormément de temps. Dans un contexte où la santé publique a été historiquement sous-financée dans de nombreux pays, le manque d'agents de santé publique suffisamment formés pour effectuer la recherche des contacts se fait ressentir. Cette situation rend un processus déjà long encore plus problématique. À l'origine de ces choix, les pouvoirs publics constatent (Islande, Singapour) ou prédisent (Belgique, France) un intérêt pour des dispositifs novateurs comme des applications de smartphone, mais aussi une adhésion insuffisante de la population au traçage numérique.

Il est intéressant de remarquer que les causes de cette insuffisance sont généralement rapportées à des problèmes d'ordre social, matériel, technologique, ou juridique et éthique. Faute de moyens ou de culture numérique, une partie de la population ne disposerait pas de la technologie requise, ou posséderait des outils numériques incapables de supporter la solution proposée. D'autres causes évoquées se rapportent à des craintes de surveillance de masse ou d'intrusion grâce aux technologies dans la vie privée. Ces facteurs sont bien évidemment à prendre en considération. Mais trop peu de contributions académiques ou de relais d'information médiatiques soulignent à ce jour l'impact des représentations et des imaginaires sociaux au travers du filtre desquels passe aussi notre effort de compréhension, en Occident, de la situation actuelle. Or, l'acceptabilité sociale d'une technologie ne repose pas seulement sur le fait qu'une technologie soit largement **accessible, efficace, explicable et** aisément employable (**intuitive**) pour un large public, **ni** sur les **précautions techniques**, **juridiques et éthiques** qui l'accompagnent. Notre niveau d'acceptabilité des outils de traçage numérique dépend aussi des référentiels, des imaginaires que nous sollicitons pour tenter de relier la crise inédite que nous rencontrons à des cadres d'interprétation qui nous sont déjà familiers (tant il est vrai que nous cherchons toujours à connaître **l'inconnu** à partir du **connu**), et des jugements de valeur sur les technologies que ces imaginaires charrient avec eux.

Autrement dit, il ne suffit pas par exemple de rendre l'interface d'une application de traçage *friendly* et intuitive, de faciliter sa compréhension et son usage pour un large public, ni de démontrer son utilité, pour garantir son acceptabilité sociale (c'est-à-dire le fait qu'un public va se l'approprier). Même l'assurance du plein respect by design des grands principes et valeurs juridiques et éthiques d'une société démocratique en matière de protection des droits individuels ne saurait suffire à elle seule pour garantir qu'une technologie sera largement employée par son public cible. Pourquoi ? Parce que nos rapports aux technologies sont aussi médiatisés par des affects et des référentiels sociaux plus ou moins favorables à leur enracinement dans nos usages quotidiens. L'humain n'entretient **pas de rapport « pur »** (au sens de « purement fonctionnel, mécanique ») aux outils technologiques. Nos relations avec la technologie sont toujours prises dans des émotions et des idéalisations. Nous adoptons une technologie en lien avec un référentiel acceptable, désirable ou rassurant (perçu, par exemple, comme ne mettant pas en danger nos biens substantiels, nos valeurs fondamentales et nos droits humains).

L'acceptabilité sociale d'une technologie ne dépend donc pas seulement de son efficacité, de son explicabilité, de sa transparence, de sa compliance juridique, de sa charte éthique, etc. Elle dépend aussi du type de « contexte d'arrière-plan » ou d'« espace imaginaire » au sein duquel cette technologie prend un sens plus ou moins **désirable**, **attractif** ou au **contraire** répulsif au sein d'une population donnée.

CONNAÎTRE LES RÉFÉRENTIELS QUI STRUCTURENT NOTRE RAISONNEMENT

Nos référentiels structurent nos compréhensions des phénomènes et notre façon de penser. Les imaginaires collectifs et les représentations sociales jouent un rôle prépondérant dans l'adhésion (l'acceptation ou le refus) des dispositifs technologiques en cette période de crise. Dès lors, il importe de rendre visibles les principaux imaginaires qui constituent les référents significatifs auxquels nous nous rapportons (plus ou moins consciemment) pour tenter de comprendre la crise que nous traversons et les solutions brandies. C'est à partir de cette explicitation que nous pouvons évaluer le niveau d'adéquation ou d'inadéquation des référentiels en présence dans la situation que nous traversons, et comprendre leurs effets sur nos relations aux technologies de traçage actuellement en débat. C'est aussi sur la base de cette explicitation que nous pouvons mettre à jour **le cadre de compréhension et de communication** le plus ajusté à la situation actuelle.

Sans prétendre à l'exhaustivité, nous pouvons distinguer au moins cinq référentiels :

1. LE RÉFÉRENTIEL DES GRANDES ÉPIDÉMIES PASSÉES
2. LE RÉFÉRENTIEL DU TEMPS DE GUERRE
3. LE RÉFÉRENTIEL DE NOTRE RELATION AVEC LA NATURE
4. LE RÉFÉRENTIEL DE LA SURVEILLANCE DE MASSE
5. LE RÉFÉRENTIEL DU SOIN

Il est donc essentiel, pour tout décideur impliqué dans des enjeux de gouvernance de technologies innovantes, de tenir attentivement compte des conditions symboliques, culturelles ou imaginaires de la réception sociale d'une technologie, s'il souhaite que celle-ci puisse rencontrer la confiance et l'adhésion d'un public cible. De telles conditions renvoient au champ des affects, des croyances et des représentations sociales. Ces significations proviennent des interprétations que des groupes sociaux (une famille, un réseau social, une association, un collectif d'entreprise, une population particulière, un groupe de populations, un pays, un continent, etc.) se donnent d'une technologie à partir de leur histoire (de leur expérience passée), de leur engagement politique et de leur culture (croyances philosophiques et religieuses, pratiques, arts, symboles, images, mythes, récits…) à un moment donné. Ces interprétations et les significations qu'elles surdéterminent d'une technologie ne sont pas arrêtées une fois pour toutes. Elles peuvent être travaillées et contestées par des contre-interprétations, des révisions de sens, des événements collectifs socialement marquants qui imposent de nouveaux cadres de compréhension. En prenant en compte le fait que ces référentiels et la construction de **ces discours vont et doivent probablement évoluer dans le temps et l'espace**.

1 LE RÉFÉRENTIEL DES GRANDES ÉPIDÉMIES PASSÉES

Le référentiel des épidémies passées réveille nos peurs ancestrales et nous pousse à surréagir, quitte à mettre en danger l'économie et les relations sociales. En effet, COVID-19 est une épidémie de dimension mondiale et d'origine virale. Elle partage ainsi un même champ de significations avec d'autres maladies virales (peste, choléra, sida, Ebola, grippe espagnole). Cela a au moins **trois conséquences pratiques** pour le moins **paradoxales**. Par son caractère et son évolution imprévisible, COVID-19 suscite de **fortes angoisses**, de la **peur**, voire des **fantasmes**. Toutefois, au regard des statistiques de mortalité (par exemple 50 millions de morts de la peste noire au XIVe siècle), le référentiel lié aux **précédentes crises épidémiques meurtrières** renvoie à des microbes dévastateurs, sans commune mesure avec la crise pandémique actuelle. Ce qui a pu conduire certains commentateurs à critiquer les réactions excessives des gouvernements ayant prononcé un confinement


+11,00.00

total, aux effets économiques sans précédent. Face à cette ambivalence, les réactions sont fortement contrastées, ce qui explique la difficulté de prédire l'adhésion ou non des citoyens à des dispositifs technologiques de suivi de sujets porteurs du virus. Cette interrogation est d'autant plus forte que le référentiel des grandes épidémies - du moins en Occident - ne renvoie pas naturellement au registre des nouvelles technologies numériques, celles-ci étant absentes des précédents exemples historiques. Dès lors, tant que les nouvelles technologies n'auront pas démontré leur **efficacité réelle en matière de santé publique** dans la crise actuelle, les attentes sociales à leur égard resteront prudentes. Ce qui explique d'ailleurs la réticence d'un certain nombre de citoyens au déploiement d'applications de traçage, en l'absence de démonstration de leur efficacité.

2 LE RÉFÉRENTIEL DU TEMPS DE GUERRE

La crise actuelle fait aussi réémerger les souvenirs des périodes de privation et de lutte en temps de guerre. Des hommes politiques de premier plan ont volontairement rapproché les deux situations pour renforcer l'unité nationale face à COVID-19. Ainsi, le 16 mars 2020 lors d'une allocution solennelle, le président Emmanuel Macron annonce aux Français : « Nous sommes en guerre ». Le 8 mai 2020, jour anniversaire de la capitulation de l'Allemagne nazie, c'est au tour de Boris Johnson, premier ministre britannique, de recourir à ce champ sémantique. Dans une lettre publique adressée aux vétérans, il compare la pandémie de coronavirus au « nouveau combat » qu'il s'agit de mener avec « le même esprit d'effort national » que 75 ans plus tôt.

La convocation du vocabulaire martial et de l'imaginaire de la guerre s'appuie sur des similitudes indéniables entre les deux situations : l'état d'urgence, l'appel à l'unité nationale, la **mobilisation** des services de santé, la convocation de l'armée, la sollicitation de toutes les forces vives, le contrôle des mouvements de population (contrôle policier, suivi par les technologies), la course aux denrées de survie (pâtes, riz, lait, farine...), la fermeture des frontières, les réquisitions de matériel par la puissance publique, les mesures d'économie de guerre (réorientation et nationalisation de certaines activités du privé aux fins de la lutte contre COVID-19). Le scénario de la crise actuelle ressemble bel et bien à un état d'exception que l'on peut retrouver déployé en temps de guerre, avec des mesures contraignantes qui touchent l'ensemble d'un pays. Mais le recours au vocabulaire guerrier est à double tranchant, car il importe avec lui, dans la situation actuelle, ses propres représentations de la technologie, non seulement comme arsenal et outil de guerre, mais aussi comme moyen de contrôle politico-idéologique des populations. Or, sommes-nous réellement en guerre contre le COVID-19 ? Les stratégies dominantes aujourd'hui ne ressemblent pas tellement à des actes de guerre, mais à des gestes de diplomatie et de prudence, comme : limiter l'exposition au virus, réduire les échanges, se confiner, rechercher la distance, archiver ses contacts, communiquer sur les chaînes de propagation pour les endiguer, porter son masque. Apprendre à vivre avec SARS-COV-2 appelle un autre art que celui de la guerre : **l'art de la cohabitation**, du **voisinage**, du **contournement**, de la **juste distance** et de la **prévenance**.

En nous inscrivant dans un paradigme de conflictualité, le référentiel de la guerre est susceptible de nous détourner de nos relations aux autres et notre relation avec la nature. Dans le contexte actuel de crise sanitaire mais aussi socioéconomique, une relation moins martiale, plus pacifique et apaisée aux technologies ne serait-elle pas plus constructive ? Le référentiel de la guerre laisse penser que nous défendre contre un ennemi suffit. Par conséquent, il comporte le danger de minimiser l'ampleur des changements organisationnels à opérer pour contenir le risque épidémique.

3 LE RÉFÉRENTIEL DE NOTRE RELATION AVEC LA NATURE

La crise actuelle nous interroge aussi sur nos relations avec la nature. Nous prenons en effet collectivement conscience qu'un développement économique sans considération pour les barrières et équilibres naturels entre les espèces est un des facteurs de la pandémie actuelle. Les observateurs soulignent la rapidité avec laquelle SARS-COV-2 s'est répandue sur la planète grâce à la globalisation des échanges économiques. On découvre que la grande majorité des victimes du COVID-19 y était prédisposée par des état de santé dégradés (maladies chroniques, affections respiratoires, obésité, tabagisme,...) en raison des habitudes de vie, des inégalités socioéconomiques et des pollutions industrielles. De ce point de vue, la cause première des décès n'est pas SARS-COV-2, mais elle

réside dans nos modes d'organisation qui se sont constitués dans l'irrespect des recommandations de santé publique, des écosystèmes naturels, des barrières entre les espèces, etc.

Ainsi, **nous ne luttons pas d'abord contre un ennemi extérieur** (la nature, les virus ne nous sont pas extérieurs), mais contre les effets de causes que nous avons nous-mêmes générées. Le référentiel de la guerre *contre* la nature n'est donc pas pertinent pour aborder des technologies dont l'objectif n'est pas de lutter contre la nature. A la différence d'un futur vaccin, qui donnera au système immunitaire les moyens de détruire un virus, les technologies de traçage ne sont pas des armes de guerre contre un fléau naturel. Elle constituent avant tout un moyen de prévention et de protection « aussi distanciée que possible » avec le virus.

Que l'humanité prenne conscience de sa responsabilité dans la crise actuelle est la première étape que ce nouveau référentiel de nos relations avec la nature nous demande de poser. La seconde étape qui s'en suit suppose, à l'instar de notre responsabilité dans le **réchauffement climatique**, une **transformation profonde des organisations** sociales, économiques et politiques à l'échelle internationale. Déterminer comment la solution technologique choisie sert la réalisation d'un futur souhaitable auquel on associe ses concitoyens / ses collaborateurs nécessite une vision qui apporte du sens au dispositif technologique et aux gestes sociaux qu'il exige de ses usagers.

4 LE RÉFÉRENTIEL DE LA SURVEILLANCE DE MASSE

Sans doute plus directement et plus fortement que le précédent, un autre référentiel impacte dans la crise actuelle la réception sociale des propositions technologiques, en particulier dans le domaine du traçage numérique : l'imaginaire de la surveillance de masse. Dès l'apparition des premières propositions d'accompagnement numérique de la sortie de crise, de très nombreuses personnalités du monde académique et de la société civile ont pris part au débat public pour mettre en garde contre la menace que constituerait tout projet technologique de traçage numérique des mouvements de population pour les principes démocratiques, l'État de droit et les libertés fondamentales. Une conséquence directe du référentiel des sociétés de surveillance de masse (récemment encore avec les affaires Snowden ou Cambridge Analytica) correspond à la polarisation du débat sur des aspects de *privacy*, au détriment d'autres enjeux éthiques.

Cette insistance sur les risques de dérives possibles et d'affaiblissement des droits et libertés fondamentales que comporterait tout recours aux technologies numériques s'accompagne souvent d'un ou deux arguments bien connus des bioéthiciens, des logiciens et des philosophes : l'argument de la pente glissante et l'argument néo-luddiste.

L'argument de la pente glissante est un type de raisonnement qui postule qu'à partir d'une prémisse donnée (la mise en place d'applications de traçage), il s'en suit avec une certaine probabilité (version honnête de l'argument), ou au contraire nécessairement (version malhonnête de l'argument), un ensemble d'effets conduisant vers une conclusion que personne ne souhaite (le remplacement d'un État démocratique par un État autoritaire et liberticide, par exemple). Cet argument devient malhonnête lorsqu'il néglige qu'un ensemble de dispositifs démocratiques permettent de réduire sérieusement les risques de dérapages des technologies envisagées : cadres juridiques et éthiques stricts, contrôles externes, évaluation continue par les usagers, etc. Quant à **l'argument néo-luddiste**, il postule que tout projet de résolution d'un problème humain par une technologie est de nature solutionniste : il fétichiserait la solution technique au détriment de la considération d'une solution plus humaine, sociale, politique et éthique. Un tel argument est aussi problématique, car il présuppose que l'outil technologique ne pourrait être un moyen parmi d'autres d'une solution plus globale, comme si l'un et l'autre s'excluaient d'emblée, ce qui est faux.

Le référentiel de la surveillance de masse est à rattacher au cadre législatif et politique dans lequel s'inscrit tout projet de déploiement des dispositifs technologiques. En effet, c'est sur fond d'état d'urgence ou de lois d'exceptions pour faire face à la crise sanitaire que repose (et reposera) la mise en œuvre de tels dispositifs technologiques. Dans ce contexte, nombre d'observateurs sollicitent à nouveau l'argument de la pente glissante pour mettre en garde contre la probabilité de voir certaines dispositions exceptionnelles tôt ou tard normalisées, bien que votées dans des circonstances

marquées par l'urgence. Ces observateurs créditent leurs alertes de l'expérience passée des états d'urgence promulgués pour faire face au terrorisme. Ils rappellent que des **lois exceptionnelles ont été normalisées dans le droit commun** à l'occasion de ces circonstances.

Ceci étant dit, si en recourant à des outils de traçage numérique, la crainte de dérives liberticides de la part des États ou dans les entreprises demeure vivante en vertu des symboles historiques qu'elle réactive (totalitarismes, autoritarismes,...), cette peur peut, dans certains cas, sous-estimer la force de nos mécanismes institutionnels (éthiques, juridiques et politiques) de protection des droits et libertés fondamentales. Nos démocraties se sont en effet dotées depuis la seconde moitié du XX^{e} siècle de solides outils de contrôle démocratique pour se protéger des dérives idéologiques toujours possibles qui pourraient pervertir leur nature. Si le risque de résurgence de politiques liberticides n'est jamais nul, l'exercice d'une surveillance d'État renforcée en régime d'exception ne signifie donc pas que nous ayons renoncé à nos valeurs et ouvert la porte à toutes les dérives. Ce sophisme culturel opère par ailleurs une réduction du sens de la surveillance et du traçage numérique. La surveillance n'est pas toujours « menaçante » ni « mauvaise ».

Avant d'être détournée de ses fins par les totalitarismes du siècle dernier, la surveillance s'est en effet instituée au sens moderne du terme entre les XVI^e^ et XIX^e^ siècles. Or, ce n'est pas un hasard si la formation du terme dans la langue française concorde sur cette période avec la naissance progressive de l'État de droit. « Surveiller » s'est forgé au XVI^e^ siècle à partir du verbe « veiller » qui signifie « rester en éveil (pour intervenir en cas de besoin) », « rester vigilant », et du préfixe « sur » qui indique l'excès ou la supériorité. Surveiller, c'est en ce sens « protéger » plus « petit » que soi, « mettre à l'abri du danger ». L'usage du verbe s'est ensuite généralisé aux XVIII^e^ et XIX^e^ siècles, donnant naissance au mot « surveillance ». **Au sens positif** du terme (**veiller sur**), la **surveillance** tient pour fonction de garantir un espace de sécurité. Elle constitue un **moyen légitime** d'assurer l'ordre public et un devoir confié dès ses origines à l'État de droit, qui se doit de garantir aux citoyens leur protection et les meilleures conditions possibles d'exercice de leurs droits et libertés fondamentales.

Les mêmes nuances valent aussi pour les moyens de la surveillance : les technologies de traçage numérique ne conduisent pas nécessairement non plus à **l'autoritarisme** ou au **totalitarisme**. L'exercice de la surveillance par de tels moyens produit en effet de nombreux bénéfices sociaux. Combien de personnes en danger, bloquées en montagne ou perdues dans un environnement méconnu n'ont pas été secourues grâce au bornage téléphonique ou l'activation du GPS de leur smartphone ? Combien de crimes de diverses natures n'ont-ils pu être déjoués grâce aux informations numériques ? Dans certaines configurations, le traçage numérique peut offrir des garanties de protection et de secours sans équivalent dans l'Histoire. Sous certaines conditions prévues par la loi, les possibilités médicales de suivi des patients et de leurs paramètres physiologiques offrent également des perspectives thérapeutiques formidables dans le champ de la médecine personnalisée. Les outils de traçage numérique donnent à de très nombreux sportifs la possibilité de mesurer leurs performances en temps réel, de programmer des entraînements de course adaptés, d'évaluer leur progression sur la base d'indicateurs bio et physiologiques de plus en plus précis. A l'échelle d'une ville, il offre la possibilité d'optimiser l'organisation des infrastructures en fonction de l'analyse des déplacements de foules, du trafic routier, etc. Mais il est vrai que le traçage numérique comporte aussi de nombreuses dérives possibles : perte de l'intimité et de la vie privée, divulgation des données personnelles, utilisation non éthique de données sensibles à son insu, commercialisation des données de santé, vol de données, piratage des outils numériques, stigmatisation de certaines catégories de population, abus de pouvoir des autorités publiques…

Au regard de ces différents exemples, les technologies de traçage numérique sont donc capables du meilleur comme du pire, et il n'existe pas de lien de consécution nécessaire qui les destinerait à un avenir

néfaste pour l'humanité. Un encadrement politique, législatif et éthique soucieux de la protection des valeurs démocratiques et des libertés fondamentales doit constituer une protection efficace contre les risques de mésusage des technologies de traçage numérique afin que leurs inconvénients soient minimisés et leurs bénéfices maximisés. Pour nous assurer que nous nous orientons davantage vers l'amélioration des aspects bénéfiques de la « surveillance » pour les individus et le public (par exemple, le suivi des maladies, la stimulation des comportements), nous avons besoin d'un contrat social explicite et public. Ceux qui sont surveillés doivent être capables de comprendre à la fois l'étendue et les limites de la surveillance, s'ils doivent accepter cette surveillance. Les acteurs étatiques et les entreprises doivent également l'accepter, même au point de limiter certains types de surveillance qui seraient « efficaces » ou « efficients » parce qu'ils ne sont pas socialement acceptables.

5 LE RÉFÉRENTIEL DU SOIN

De nombreux référentiels, nous l'avons vu, sont sollicités dans la crise pour lui donner des sens divers et proposer des pistes d'action correspondant aux imaginaires mobilisés. Certains de ces référentiels ont pu paraître plus adéquats que d'autres. Mais la visée qui mobilise la grande majorité des énergies et espoirs des citoyens dans la réalité actuelle demeure néanmoins d'une autre nature.

Car nous ne sommes pas réellement en guerre, confrontés à un enjeu de défense où l'ennemi est extérieur à la Nation, ou mettant en danger la stabilité de l'État. Nous ne sommes pas non plus dans un état d'urgence antiterroriste, face à un enjeu de sécurité où l'ennemi est identifiable à certaines catégories spécifiques de la population, ou à certains profils. Nous sommes davantage dans une situation où chacun est potentiellement un risque et un soutien pour autrui, où chacun est appelé à la responsabilité pour soi et pour autrui. Nos préoccupations présentes, liées au « fait social total » que nous expérimentons actuellement (v. Annexe n° 1), n'ont pas été non plus suscitées par des pratiques de surveillance inacceptables mais par l'expansion d'une pandémie et ses multiples effets sociaux, économiques, politiques. Nous ne sommes enfin pas mobilisés en première ligne par des pourparlers avec la nature en vue d'une nouvelle alliance, comme dans le cas de la problématique du changement climatique. Nous sommes plutôt dans un **enjeu de santé publique** qui met en jeu la préservation d'un bien commun, la santé, que nous cherchons à maintenir pour le plus grand nombre, en particulier celles et ceux d'entre nous qui sont les plus exposés aux morbidités de la COVID-19.

Si l'état d'urgence sanitaire entretient des similitudes avec d'autres états d'exception dans les moyens sollicités, la fin est donc très différente, et l'esprit des mesures l'est aussi. En prendre conscience est essentiel pour ne pas se tromper de discours, d'horizon imaginaire, et de visée. Confrontés avec la pandémie à un enjeu de santé publique, nous ne sommes pas en guerre, nous sommes *en care*, et *en besoin de care* avant tout autre référentiel mobilisable, avant tout registre d'actions parallèle, compatible ou complémentaire avec nos besoins dans la situation présente.

La crise nous rappelle en effet notre **vulnérabilité** et notre **interdépendance** fondamentales. Elle nous fait prendre conscience dans nos confinements et ses conséquences multiples, que nous dépendons toutes et tous des attentions et du soin d'un nombre incalculable d'acteurs privés et publics qui, dans tous les registres de la vie en société, nous permettent de continuer à vivre. La situation actuelle souligne plus que jamais la valeur d'un « prendre soin de soi, d'autrui et du monde », qui traverse les frontières du privé et du public, et interpelle profondément la façon dont nous mènerons à l'avenir nos activités humaines : sommes-nous prêts à les exercer avec plus de soin ?

Il est important de souligner ici que cet appel au *care* n'est pas réductible à l'univers médical et à l'engagement sans faille de nos soignantes et soignants, même si ces derniers l'inspirent, en font bien évidemment partie et occupent dans la gestion de la pandémie un rôle essentiel. **La référence *au care* dans la crise implique une conception du soin beaucoup plus large, dont le soin médical n'est qu'une des expressions**, et qui se manifeste dans tout ce que nous aimerions faire (et faisons déjà) pour rendre notre « monde » **habitable** (monde qui comprend nos corps, nos environnements sociaux, culturels et techniques, nos relations avec la nature), de telle sorte que nous puissions y vivre et nous y épanouir autant que possible. Le soin est en ce sens tout autant une visée qu'un ensemble de dispositions subjectives et de pratiques particulières dont l'œuvre est de soutenir,

entretenir, protéger, permettre l'épanouissement d'un monde humain, et de toutes celles et ceux qui l'habitent.

Ce besoin de *care* rejoint aussi un besoin de justice qui s'exprime dans les populations, face aux risques de nouvelles situations d'inégalités et de discriminations que la gouvernance de la crise pourrait créer, notamment en recourant à certaines technologies de traçage en situation d'urgence et d'impréparation démocratique. **Il ne peut enfin y avoir de politique du soin sans l'inclusion et la participation de toutes les parties prenantes du soin.** Tout souci de soi, des autres et du monde, présuppose toujours l'exercice d'un ensemble de compétences toujours particulières, souvent apprises d'expérience et adaptées aux enjeux de situations précises (parentales, sociales, éducatives, environnementales, culturelles…). Ces pratiques s'inscrivent elles-mêmes dans des institutions très diverses, dans des procédures d'évaluation, dans des contrats d'objectifs, dans des politiques locales et des cultures concrètes.

Au-delà de la période particulière qui a été celle du confinement et de la mise en place des stratégies de santé publique nécessaires pour éviter l'effondrement des systèmes de santé de nombreux pays, la référence au soin dans la situation actuelle appelle plus que jamais le développement d'une politique du soin ambitieuse et des conditions d'une société plus juste. Mais le soin ne doit pas se limiter à son acception biomédicale, il doit englober des considérations sociales, politiques, économiques bien plus larges.

Une éthique du soin demande de celles et ceux qui s'en réclament une transparence, une sincérité et une cohérence fortes, conditions nécessaires du respect de tout contrat social, ainsi que de la dignité et des droits de la personne humaine. Face aux risques toujours possibles de transgression du contrat social, le respect d'une politique du soin demande non seulement de bien **comprendre les technologies** envisagées dans la crise actuelle (Partie II du rapport), mais aussi de se doter d'une **gouvernance inclusive** et d'un **outil d'évaluation technique, juridique et éthique approprié des technologies** (Partie III du rapport). Toute technologie numérique de soutien à la sortie de crise ne devrait être en effet mise en oeuvre qu'à la condition que sa conception et son usage fassent l'objet d'une évaluation rigoureuse par des instances indépendantes représentatives de la société civile, selon des processus qui garantissent la conformité de la technologie aux termes du contrat social et aux principes et valeurs démocratiques auxquels tout un chacun tient face à la crise.

Dans la perspective d'une politique du soin en temps de crise, l'idéal de gouvernance inclusive et l'outil d'évaluation multidimensionnel des technologies numériques qui seront développés plus loin dans ce rapport constituent un binôme complémentaire et nécessaire, qui devraient s'incarner avec souplesse selon les réalités du terrain, tant au niveau des entreprises, des corps intermédiaires ou de l'État que dans leurs interactions.

RECOMMANDATIONS

Dans un objectif partagé de lutte contre le COVID-19 et de reprise des activités sociales, culturelles et économiques, cette section qui s'achève sur les référentiels de la crise était un prérequis incontournable. Si les enjeux de la crise actuelle sont multiples, elle a montré en effet qu'ils relèvent aussi d'un **conflit des imaginaires**. Tout décideur, tout collectif doit être capable de parler avec justesse des situations problématiques rencontrées, s'il espère leur trouver quelque solution adaptée. Dans ce but, il est essentiel de **savoir quel référentiel**, quel registre de signification **solliciter**, et quelles sont les **conséquences ou implications** (bénéfices et limites) d'un tel choix.

Dans ce contexte actuel où les dispositifs technologiques sont corrélés dans l'opinion publique, parfois à un référentiel de la surveillance, parfois à celui de la guerre ou encore du terrorisme, la question de la **temporalité** paraît décisive pour tout décideur. Pour un gouvernement, il s'agira de déterminer les **critères définissant un état d'urgence**, les circonstances permettant de lever les mesures d'exception mises en place pendant une crise, et celles permettant de réactiver des mesures d'exception afin de prévenir une nouvelle épidémie. Pour une entreprise, il s'agira de veiller à ne pas laisser perdurer ces pratiques de contrôle d'accès à des locaux ou de gestion de l'espace privé du lieu de travail après la crise. Au risque de créer de la **défiance** et de glisser vers une forme d'état d'exception qui deviendrait ou serait perçu comme permanent.

Le danger serait en effet de tomber dans une **banalisation** progressive de l'usage des technologies de traçage et dans **l'accoutumance** du suivi des citoyens et des salariés. Les référentiels que nous avons parcourus font prendre conscience de l'impact qu'ils peuvent avoir sur nos perceptions et nos décisions. La prise en compte de leur existence peut ainsi informer gouvernements comme entreprises sur le choix des technologies et des modes de gouvernance adéquats.

Penser la situation actuelle à partir du référentiel du soin, qui nous semble le plus approprié pour l'enjeu de santé publique que nous traversons et pour les défis sociétaux plus larges qu'il soulève, implique de fonder les stratégies de sortie de crise sur des principes de **gouvernance inclusive**, de **dialogue**, de **solidarité** et **d'équité**, de **responsabilisation** et de **confiance**. Contrairement à l'idée qui nous laisserait penser que la responsabilité de nous défendre incombe à l'État et que le danger nous est extérieur (alors que nous pouvons tous être porteurs du virus), un tel référentiel appelle la recherche incessante d'un juste compromis entre le besoin de liberté de choix des individus (autonomie) et la responsabilité au soin de chacun pour autrui (santé), tout en accordant une priorité sans condition à la protection des populations les plus vulnérables.

CHAPITRE 2

COMPRENDRE LES CARACTÉRISTIQUES DES TECHNOLOGIES

La sélection d'une technologie pour résoudre un problème de société n'est **jamais neutre**. Non pas du fait de la technologie elle-même mais plutôt de par les conditions d'acceptabilité et de gouvernance que leur emploi efficace et proportionné impose.

Dans cette perspective, quatre **finalités** des dispositifs technologiques de sortie de crise et de relance de l'activité ont été analysées : **1) le traçage** des individus porteurs du virus, **2) l'étude des comportements** à l'échelle collective, **3) le contrôle du respect** des mesures sanitaires, **4) le contrôle d'accès** à des espaces privés.

Pour chacun de ces axes, les **choix des architectures techniques et des modes de gouvernance des dispositifs se révèlent étroitement liés**, et c'est sur cet ensemble indissociable que le décideur, public ou privé, doit statuer .

Une dizaine d'applications de traçage développées à travers le monde ont ainsi été analysées et discutées. Les **risques** que ces technologies pourraient présenter ont également été évoqués, ainsi que les **options envisageables pour les atténuer**. Ces considérations pourront accompagner le décideur dans l'**arbitrage** à opérer au sein d'un contexte éminemment complexe et dicté par l'urgence.

De ces travaux ressortent notamment d'importants défis liés à **la nature et à la précision des données** collectées (les données de localisation **GPS** vs les données de proximité **Bluetooth**), à l'**interopérabilité** des applications tant aux niveaux national qu'international, et à l'**interdépendance** avec des systèmes tiers.

Un débat important, voire souvent virulent, concerne le choix entre un système **centralisé** et **décentralisé**. Notre analyse montre que **cette apparente dichotomie** est en réalité à nuancer : de nombreux dispositifs sont hybrides, intégrant à la fois des composants centralisés et décentralisés. Il s'agit toutefois d'une décision particulièrement **structurante**, en ce qui concerne tant les mesures de sécurité informatique et de respect du droits des individus que les modalités de gouvernance.

Selon plusieurs études et publications récentes, plus d'une quarantaine d'applications de traçage de suivi de contacts ont été développées ou déployées dans plus d'une vingtaine de pays. Des mesures alternatives de suivi numérique des individus (bracelets, caméras) et de technologies de surveillance (de mouvement ou de température corporel) de population seraient, quant à elles, actives dans une trentaine de pays. Ces développements sont parfois le résultat d'initiatives privées, parfois le fait d'organismes indépendants sans but lucratif, ou d'initiatives soutenues activement par les pouvoirs publics. Au total, c'est donc aujourd'hui dans plus d'une cinquantaine de pays que sont développées, selon des modalités très différentes, des techniques de gestion et de contrôle de la crise sanitaire par le moyen d'un outil numérique. Dans ce contexte, notre rapport propose une typologie des dispositifs technologiques pour une sortie de crise sanitaire. Il en expose les principales caractéristiques techniques, afin d'illustrer leur influence sur les modes de gouvernance et alerter tout décideur public ou privé sur l'importance du choix technologique et l'impact que celui-ci peut avoir sur la société, son administration, son entreprise et leur organisation.

TYPOLOGIE DES DISPOSITIFS TECHNOLOGIQUES POUR LUTTER CONTRE LA COVID-19

L'attention et les débats internationaux se sont jusqu'à présent particulièrement concentrés sur **les applications de traçage** étudiées par les gouvernements. Il convient toutefois d'avoir à l'esprit l'ensemble des technologies pouvant être utilisées dans un contexte de sortie de crise sanitaire. En particulier, d'importants enjeux se présenteront **pour les entreprises** qui choisiront de déployer en leur sein des outils de suivi des états de santé de leurs salariés, que ce soit par la collecte de **données de santé**, le traitement de **données de déplacement** ou l'incitation (voire l'obligation) de recourir à l'usage d'un dispositif technologique.

Face à la prolifération de ces outils, de multiples classifications seraient possibles. Nous avons choisi une typologie consistant à distinguer principalement les quatre grands axes de dispositifs technologiques suivants :

1. LE TRAÇAGE DES INDIVIDUS PORTEURS DU VIRUS
2. L'ÉTUDE DES COMPORTEMENTS À L'ÉCHELLE COLLECTIVE
3. LE CONTRÔLE DU RESPECT DES MESURES SANITAIRES
4. LE CONTRÔLE D'ACCÈS À DES ESPACES PRIVÉS

Le schéma ci-dessous présente ainsi les différentes finalités associées à chacun de ces axes ainsi que les techniques pouvant être utilisées.

Typologie	Traçage des individus porteurs du virus	Étude des pratiques collectives	Contrôle du respect des mesures sanitaires	Contrôle de l'accès à des espaces privés
Exemple	Contact tracing	Cartographie des déplacements de population	Bracelet électronique virtuel de détection des symptômes	Contrôle de l'accès aux lieux de travail, à des commerces
Finalités	· Aviser automatiquement les personnes ayant rencontré une personne testée positive pour permettre aux personnes à risque de gérer leur isolement · Identifier les principaux vecteurs de contamination pour prendre les mesures adéquates · Aviser les propriétaires immobiliers et les employeurs du fait qu'une ou des personnes testées positives ont été sur les lieux, et de gérer les cas nécessitant des fermetures d'immeubles ou de lieu de travail · Améliorer la compréhension des facteurs de risques et des probabilités de contagion sur une base individuelle	· Informer en temps réel de la propagation du virus · Anticiper les fluctuations de population pour adapter les besoins en ressources (par exemple au sein des hôpitaux) · Mesurer l'efficacité des mesures de politiques publiques mises en œuvre · Surveiller les concentrations anormales de population dans des espaces publics, afin de pouvoir y réagir efficacement · Améliorer la compréhension des facteurs de risques et des probabilités de contagion sur une base collective	· Contrôler le respect des mesures de confinement par les individus concernés · Mesurer l'efficacité des règles de conformité · Limiter les déplacements et voyages non autorisés · Identifier les symptômes avec précision et proposer des solutions de détection efficaces · Assister les individus par une aide médicale	· Aider l'employeur dans son devoir de préserver la sécurité de ses employés · Permettre la reprise de l'activité · Éviter que sa chaîne de production ou que son lieu de travail ne véhicule (au sein de son entreprise, ses partenaires économiques et ses clients) le virus · Réguler, autoriser ou interdire l'accès à un magasin, commerce, espace privé, etc. · Évaluer le risque personnel pourrait être utilisé pour l'employeur pour gérer les cas d'exclusion des lieux de travail
Techniques utilisées	· Bluetooth · GPS · Ultrasons · Bornage téléphonique · Vidéosurveillance	· Bornage téléphonique · GPS · Cartes bancaires · Réseaux sociaux	· Capteurs/ IoT · GPS · QR Code · Drones · Systèmes d'IA	· Caméra thermique · Reconnaissance faciale · Chatbot · Usages blockchain · Objets connectés · Systèmes IA

Les exemples pour chacune de ces quatre catégories sont nombreux. Il ne s'agit pas ici d'en faire une liste exhaustive, mais d'en illustrer la diversité et d'en présenter les principales caractéristiques.

1 LE TRAÇAGE DES INDIVIDUS PORTEURS DU VIRUS

Au titre de ce rapport, nous avons notamment étudié en profondeur plusieurs initiatives de la première catégorie, dite de traçage. En particulier les initiatives **DP3T**, **TraceTogether**, **COVI App**, **ROBERT**, **Apple/Google API**, **Aarogya Setu**, **COALITION**, ou encore **NHSx**, à partir de la documentation accessible au public en ligne. Un tableau comparatif de ces projets est annexé au présent rapport (voir Annexe n° 3), ainsi que des analyses plus spécifiques (voir Annexe n° 4). La grande majorité de ces initiatives collectent des données personnelles par le recours à la technologie **Bluetooth** (certains utilisent également des données GPS), utilisent des mesures techniques de chiffrement (majoritairement pour les données « au repos », parfois également pour les données « en transit », à savoir pendant qu'elles sont acheminées) et de pseudonymisation des données.

Il convient d'observer que de nombreuses publications évoquent le caractère anonyme des données collectées, ce qui mérite d'être largement tempéré. D'une part, parce que la définition d'une **donnée personnelle** varie d'un continent à un autre (voir par exemple la différence entre *personal data* vs *personally identifiable information - PII*). D'autre part, parce que les standards pour reconnaître le caractère anonymisant d'une donnée n'est pas non plus homogène d'un pays à un autre, si bien que certains parlent d'informations **anonymisées**, ce qui supposerait qu'il soit irréversiblement impossible de **re-identifier** un individu, alors qu'il s'agit la plupart du temps d'informations simplement **pseudonymisées**, c'est-à-dire d'informations pour lesquelles l'identification de la personne concernée est techniquement toujours possible. Tout décideur doit donc être conscient qu'en déployant ces solutions, les données traitées le seront très certainement sous forme personnelle et non anonymisée. Enfin, certaines données peuvent à premier abord ne pas paraître **sensibles**. C'est le cas des notifications transmises aux personnes considérées infectées. Néanmoins, il convient de noter que le simple fait de notifier un individu pourrait potentiellement être considéré en soi comme une donnée de santé (à ce sujet voir en particulier Annexe n° 4).

Plusieurs distinctions méritent ensuite d'être précisées. Tout d'abord, la différence entre un **protocole** et une **application**. Un protocole correspond à un ensemble de règles qui régissent le fonctionnement d'un outil (que ce soit une application, un objet connecté, etc.). Ainsi, un protocole définit les règles et les procédures permettant à des processus informatiques d'échanger des données. Une application est, quant à elle, un ensemble logiciel utilisé pour la réalisation d'une tâche. Une app s'exécute en utilisant un système d'exploitation (par exemple l'OS, *Operating System*, d'un ordinateur ou d'un smartphone) et suivant les règles de plusieurs protocoles. À titre d'exemple donc, l'application StopCovid repose sur le protocole ROBERT. Mais StopCovid aurait aussi pu choisir de reposer sur le protocole DP3T. Inversement, le protocole BlueTrace a été utilisé à Singapour par l'application TraceTogether, mais également par le gouvernement australien, lequel a développé sa propre application COVIDSafe, prenant justement en compte les retours d'expérience de l'application singapourienne.

Sans entrer dans des considérations trop techniques, il convient également de distinguer les applications des **API** (*Application Programming Interface*) qui sont des interfaces de programmation permettant à une entité informatique d'interagir avec des systèmes tiers. Se pose dès lors d'importantes questions de dépendance. En effet, l'**interdépendance** des applications vis-à-vis de systèmes tiers expose techniquement à des possibilités d'accès aux données stockées dans l'application. Tout aussi sensible est l'enjeu d'**interopérabilité**. Par exemple, Apple et Google proposent conjointement une API uniquement compatible avec les applications qui reposent sur des systèmes décentralisés. Cette API permet d'utiliser les applications de traçage sur des smartphones équipés de systèmes d'exploitation Android (Google) et iOS (Apple), tout en préservant la vie privée des utilisateurs. La question de l'interopérabilité entre les systèmes est fondamentale et a déjà suscité de nombreuses polémiques dans certains pays comme en France (où le protocole ROBERT considéré comme centralisé n'est en l'état pas compatible avec l'API Apple/Google). L'application développée par NHSx - qui a longtemps hésité entre une approche centralisée et décentralisée - pourrait rencontrer des problèmes similaires.

Une autre distinction importante doit être réalisée entre une **technologie** et **son usage**. Les débats sur le fait de savoir si ces dispositifs devraient être déployés sur une base obligatoire ou volontaire renvoient au contexte, à la fois législatif et politique,

de déploiement d'une technologie, mais pas à la technologie elle-même. Par conséquent, ni un protocole ni une application ne sont « obligatoires » en soi, seul leur usage le sera ou non. Tout dépend donc du **contexte** de sa mise en oeuvre. Ainsi, une même application pourrait être obligatoire dans un pays et facultative dans un autre. En Inde, l'application Aarogya Setu fait partie des rares initiatives à avoir été rendues obligatoires, sous peine de sanction pénale (le gouvernement ayant changé de position par la suite).

Par ailleurs, lorsqu'un outil est destiné à être utilisé par des gouvernements et entreprises du monde entier, il existe un risque inhérent pour les citoyens et employés résidant dans des pays qui n'ont pas de lois et de réglementations en matière de protection des données, de sécurité sur le lieu de travail, ou contre la discrimination. Par exemple, alors que certains pays comme l'Australie ont déjà modifié leur législation nationale en matière de protection de la vie privée afin d'introduire des dispositions spécifiques prévoyant que l'autorité nationale de protection de

la vie privée - le Bureau du commissaire australien à l'information (OAIC) - exerce un contrôle sur les données de l'application ; établissant un processus de suppression des données à la fin de la pandémie ; et exigeant que le ministre de la santé et l'OAIC soumettent des rapports concernant l'application ; d'autres pays n'ont actuellement aucune loi d'application générale qui s'appliquerait à la collecte, à l'utilisation et à la divulgation de renseignements personnels par le biais d'applications de recherche de contacts ; et d'autres encore ne disposent pas d'un corpus législatif garantissant le respect des droits fondamentaux.

Dès lors, on comprend l'importance d'utiliser, autant que possible, des dispositifs technologiques qui soient par défaut et par conception protecteurs des libertés individuelles et des droits fondamentaux. En revanche, on comprend également que l'efficacité ou les mesures techniques d'un dispositif pourront parfois être insuffisantes, notamment lorsque leurs usages ne sont pas encadrés par des dispositions législatives ou réglementaires suffisamment protectrices.

Les aspects culturels de nos rapports aux technologies ne doivent pas non plus être sous-estimés. À ce titre, Singapour est un pays socialement cohésif, c'est-à-dire une société avec un degré de confiance élevé dans le gouvernement. Dès lors, TraceTogether et d'autres applications basées sur le protocole BlueTrace pourraient avoir du mal à obtenir l'adhésion générale nécessaire à son efficacité dans des juridictions qui ne partagent pas ces caractéristiques. Pour ces pays, le déploiement d'une telle application serait alors certainement accompagné de réglementations obligatoires afin d'atteindre les bénéfices sociétaux attendus.

Enfin, la question de la **véracité** et **vérifiabilité** de l'infection par SARS-COV-2, peu évoquée dans la littérature, constitue un critère de choix important. Parmi la dizaine d'initiatives étudiées, deux types d'approche existent à proportion égale : l'auto-diagnostic versus le diagnostic vérifié. Ainsi, l'initiative TraceTogether fonctionne sur la base d'un diagnostic vérifié, impliquant une procédure de vérification du dépistage via des agents gouvernementaux responsables du suivi des contacts, ce qui permet d'exploiter des données plus précises. A l'inverse, l'auto-diagnostic (comme pour NHSx ou encore COALITION) implique uniquement la prise en compte de symptômes, sans qu'un diagnostic médical intervienne, ce qui augmente les probabilités de faux positifs. Le recours à une application fondée sur l'auto-diagnostic dépendra aussi de la relative facilité ou difficulté d'accès aux tests de dépistage, conditionnant l'obtention d'une confirmation médicale d'infection. Dans tous les cas, il existe une crainte légitime qu'un dispositif technologique puisse fournir, sous forme numérique, un **score de risque**, en ce que cela contribuerait à créer un sentiment de panique chez un utilisateur ayant un score élevé. Sur cet aspect, le choix technologique de COVI-App développé est intéressant. En effet, l'application est configurée de manière à fournir des informations et des **recommandations**, plutôt qu'un simple score brut ininterprétable. Au lieu de fournir une évaluation binaire (oui/non) à la question de savoir si la personne a été en contact avec une autre personne diagnostiquée COVID-19, la solution de *machine learning* COVI-App développée par le MILA calcule la probabilité globale d'exposition des utilisateurs à COVID-19 (le *risk score*), sur la base des informations démographiques, sanitaires et comportementales fournies par l'utilisateur, des diagnostics officiels, s'ils sont disponibles, et du risque des autres utilisateurs du réseau. Ce choix technologique vise à responsabiliser les utilisateurs, en les mettant en mesure d'adopter les comportements appropriés en fonction de leur niveau de risque.

2 L'ÉTUDES DES COMPORTEMENTS À L'ÉCHELLE COLLECTIVE

Il existe une **deuxième catégorie** de dispositifs technologiques, dont l'objet est d'**analyser les comportements**, non pas à l'échelle individuelle comme pour les application de traçage, mais à **l'échelle collective**. Il ne s'agit plus là de traitement de données personnelles, mais d'informations **statistiques agrégées**. Cette pratique se retrouve sur plusieurs continents. Aux États-Unis, des chercheurs ont ainsi pu utiliser les données de localisation des utilisateurs Facebook qui partagent leur historique de localisation pour développer des cartes mesurant la distanciation physique. En Chine, l'entreprise Baidu a utilisé son service de cartographie pour modéliser en temps réel les zones contagieuses. En Finlande, l'opérateur télécom Telia partage les données cellulaires de localisation anonymisées au gouvernement pour permettre un suivi des mouvements de population et prévenir les zones à risque.

Dans certains cas, ces pratiques sont réalisées par l'utilisation des **données de bornage téléphonique,** lesquelles transmettent des informations issues des appareils mobiles, sans besoin d'une activation quelconque par les utilisateurs. Dans d'autres cas, le traitement de **données GPS** issues d'applications mobiles nécessite une activation par l'utilisateur. Les données sont agrégées et servent à établir des rapports de fréquentations. Dans des hypothèses plus résiduelles, **le système de cartes bancaires permet de retracer les lieux de transaction** et permet en agrégeant les données d'avoir une carte des déplacements.

3 LE CONTRÔLE DU RESPECT DES MESURES SANITAIRES

Une **troisième catégorie** de technologies concerne les **objets connectés** qui facilitent le suivi de l'état des personnes et le contrôle du respect des **mesures de confinement**. Sans prétendre encore une fois en réaliser une liste exhaustive, nous en citons quelques-unes pour témoigner la diversité des approches. En Australie, certaines personnes mises en quarantaine pourront être suivies par l'installation d'une caméra à leur domicile ou devront porter un bracelet électronique. En Pologne, les personnes confinées sont invitées à télécharger une application qui leur impose d'enregistrer un selfie géolocalisé. Des agents vérifient ensuite que ces personnes sont bien à leur domicile via l'envoi de messages et l'analyse des données de localisation. À Hong Kong, les personnes confinées se voient obligées de porter un bracelet électronique qui, couplé à une application, permet aux autorités de vérifier le respect de la quarantaine. À Taïwan, des fonctionnaires appellent deux fois par jour les personnes assignées à résidence lesquelles s'exposent à une publication de leur identité et à 30 000 € d'amende en cas d'absence. En Russie, le gouvernement utilise des caméras couplées à un système de reconnaissance faciale, ainsi que les données de localisation de téléphones pour surveiller les personnes placées en quarantaine.

Ce rapport s'est intéressé à une approche innovante lancée en Allemagne par l'Institut Robert Koch (RKI pour **Robert-Koch-Institut**). L'agence fédérale allemande pour la santé publique a publié une application de « don » de données, nommée **Corona-Datenspende**. L'application RKI est conçue pour que les utilisateurs fassent don à l'agence des données de santé provenant de leurs vêtements, bracelets et applications de bien-être. L'objectif est de tirer de ces données des informations sur la diffusion de COVID-19 à l'échelle nationale et régionale. Notre rapport a étudié plus spécifiquement cette initiative qui présente la particularité d'améliorer les possibilités de prédiction de la propagation de COVID-19 à l'échelle nationale sur la base de données sanitaires non spécifiques (telles que le pouls) et, par conséquent, d'accélérer et de cibler les futures mesures de confinement dans les zones identifiées à haut risque. Cela étant dit, le projet cherche à servir la santé publique plutôt qu'à donner à l'utilisateur du don une indication sur la possibilité qu'il soit ou non infecté. Étant donné que les capacités de test sont limitées et que de nombreuses infections par COVID-19 ne présentent que des symptômes très légers (de sorte que les personnes infectées ne demanderont probablement jamais de test elles-mêmes, mais peuvent néanmoins transmettre le virus à d'autres personnes qui pourraient développer une maladie plus grave), le RKI vise à améliorer l'estimation du nombre possible d'infections par COVID-19 non détectées.

4 LE CONTRÔLE DES ACCÈS À DES ESPACES PRIVÉS

Enfin, une **quatrième catégorie** renvoie aux applications pouvant être déployées par et au sein des entreprises et des **espaces privés**. En effet, si l'attention a jusqu'à présent particulièrement été portée autour des applications pouvant être mises en oeuvre par les gouvernements et des enjeux autour du traçage, il convient d'étudier avec précaution les initiatives des entreprises privées. Celles-ci auront très certainement vocation à croître de manière importante, dans le futur, et nécessitent un examen approfondi tant elles impactent et impacteront nos manières d'être et d'agir. Dans tous les cas, les employés ne doivent pas subir l'adoption de l'outil, mais en être pleinement acteurs. L'adhésion volontaire des employés à l'outil n'en sera que facilitée.

Dans un contexte d'emploi, l'aspect « volontaire » de l'adoption de l'outil peut devoir être nuancé. Comme de nombreux autres outils utilisés dans un contexte professionnel, leur utilisation peut devenir une condition obligatoire de l'emploi, tant que le fait d'obliger les employés à utiliser les outils ne viole pas le droit applicable.

Toutefois, le fait que les employeurs puissent avoir le droit légal d'imposer l'utilisation de certaines technologies par les employés sur le lieu de travail ne signifie pas qu'ils sont « obligés » d'imposer des technologies nouvelles dotées de capacités de surveillance sans donner préalablement aux employés concernés la possibilité de participer, au moins dans une certaine mesure, au processus décisionnel lié à la sélection et au déploiement de ces outils, dans le cadre d'un processus de gouvernance inclusif, tel qu'il est examiné plus en détail dans la partie III.

Ces dispositifs visent à mesurer l'état de santé d'un employé avant de lui permettre ou de lui refuser l'accès à son lieu de travail. Ainsi, l'opérateur télécom britannique Vodafone et la société de télésurveillance Digital Barriers ont développé une caméra thermique connectée pour détecter tout employé présentant un état de fièvre. Le groupe québécois OPTEL a lancé, quant à lui, une application mobile qui vise à sécuriser les locaux. L'application permet aux employés de répondre à des questions concernant leur état de santé, par l'intermédiaire d'un agent conversationnel, et d'accéder à leur lieu de travail si l'évaluation du risque est considérée faible. En France, le Crédit Agricole et Onepoint ont travaillé de concert au développement de l'application "Copass" (badge numérique) pour gérer la reprise de l'activité des entreprises. En répondant à un questionnaire de santé, les salariés se voient attribuer un "niveau de sensibilité" relatif au COVID-19 pour aider les entreprises à établir des protocoles d'organisation (télétravail, horaires décalés…). L'entreprise ONHYS simule, quant à elle, des flux de visiteurs, d'usagers, de patients ou encore des personnels salariés au sein d'un établissement. Le logiciel teste différentes configurations d'aménagements pour identifier la solution permettant de réduire au mieux le risque des personnes. Pour assurer la distanciation physique sur le lieu de travail, Landing AI a développé un outil de détection basé sur une intelligence artificielle, qui modélise la distance entre les personnes à partir des flux vidéo en temps réel. Ce système a déjà été déployé dans les caméras de sécurité d'usines et de sites industriels.

Ce rapport a plus particulièrement étudié deux cas d'usage. Le premier, développé par l'entreprise canadienne TerraHub, est un exemple de « passeport immunitaire » basé sur la technologie blockchain, permettant aux employés de partager volontairement des données de santé, tout en modulant l'accès à celles-ci. **TerraHub** a décidé d'adapter sa solution Credential Link, pour mettre en œuvre les fonctionnalités permettant d'accélérer et

de faciliter le retour des employés après la période de confinement. Basé sur le protocole de chaîne de blocs Hyperledger Fabric, Credential Link propose au collaborateur soit de procéder quotidiennement à une auto-déclaration de son état de santé, soit de télécharger d'autres justificatifs attestant de sa capacité à retourner au travail en toute sécurité. Un algorithme produisant une synthèse de cet état est transmis à l'employeur chaque jour pour accompagner ce dernier dans la mise en place de dispositifs de sécurité.

Le second cas d'usage étudié est un objet connecté développé par l'entreprise polonaise **Estimote**. Nommé « Proof of Health », il a pour objectif de permettre aux employeurs d'anticiper la transmission du virus au sein du personnel. L'appareil comporte un bouton utilisé par les employés pour alerter la direction d'un événement (symptôme, contamination). Ce dispositif comprend un système GPS, ainsi que des capteurs de proximité alimentés par Bluetooth et une connectivité radio à bande ultra-large. L'efficacité de cette solution dépend de la déclaration par l'employé infecté et de l'apparition de symptômes. De par ses caractéristiques techno-logiques, une telle application présente un risque éthique non négligeable de tracer les déplacements de chaque employé au sein d'un bâtiment, de mesurer le temps passé à un poste de travail ainsi que les temps de pause, voire de connaître la fréquence des interactions entre les collaborateurs (et peut être même en dehors du lieu de travail ou hors des horaires de travail). Dans le cas du dispositif Estimote, aucune information relative à la sécurité ou aux données stockées sur l'appareil et sur le serveur ne semble disponible.

Dans ce contexte, il est intéressant de relever le UK Coronavirus (Safeguards) Bill 2020 qui tente de fournir des garanties appropriées en ce qui concerne les applications de suivi des symptômes et de recherche des contacts qui sont actuellement déployées au Royaume-Uni ; et qui prévoit des garanties minimales qui seront nécessaires si nous passons à un déploiement de « certificats d'immunité » (communément appelés passeports) dans un avenir proche. Il ne prescrit aucune approche technologique particulière pour la création d'applications et ne tente pas de reproduire les directives GDPR et ePrivacy. Il suggère plutôt quelques garanties de base qui doivent être ajoutées à ce que ces lois fournissent déjà.

Plus précisément, le projet de loi précise que :

(a) Personne ne sera pénalisé pour ne pas avoir de téléphone (ou autre appareil), pour quitter la maison sans téléphone, pour ne pas charger le téléphone, etc. ;

(b) Personne n'est obligé d'installer une application de recherche de symptômes et de contacts, ou de partager des messages sur son statut sur une telle application (par exemple à un employeur, un assureur ou une université) ;

(c) Les données personnelles collectées par une application ou contenues dans un certificat d'immunité ne doivent pas être partagées au-delà du NHS et des chercheurs sur les coronavirus, sauf si elles sont anonymisées de manière sécurisée ;

(d) L'anonymisation doit être certifiée par un code de conduite rigoureux ;

(e) Les données personnelles collectées par les applications ou le certificat d'immunité doivent être supprimées ou anonymisées dès que possible, ou au plus tard immédiatement après l'expiration de la période d'urgence ;

(f) Les « passeports d'immunité » ne doivent pas devenir des passeports internes nouveaux et non contrôlés, ni être utilisés par l'État ou le secteur privé pour exercer une discrimination qui ne serait ni nécessaire ni proportionnée à l'objectif social légitime de contrôle du COVID-19.

LES CARACTÉRISTIQUES TECHNIQUES INFLUENT LES MODES DE GOUVERNANCE

L'analyse des dispositifs développés pour gérer la crise sanitaire montre que **le choix des architectures technologiques influe directement sur leur mode de gouvernance** : le type de technologies utilisées, les modalités de stockage des données, le choix d'une infrastructure centralisée ou non ont un impact sur l'ensemble du projet et sur son acceptation sociale. L'adage du professeur Lawrence Lessig « *code is law* » est plus que jamais d'actualité. Certaines caractéristiques techniques clés doivent donc être connues de tout décideur ayant à évaluer et choisir un dispositif technologique, dans le secteur public ou en entreprise.

A l'heure actuelle, les applications de suivi de contact (*contact tracing*) ont fait l'objet des plus vifs débats publics. Les informations relatives à leurs caractéristiques techniques sont les plus facilement consultables, certaines étant parfois accessibles sous forme de documentation *open source*. Nous avons donc décidé d'utiliser le cas de ces applications pour mettre en avant les questions de gouvernance qu'elles suscitent et d'illustrer les enjeux soulevés par le déploiement des dispositifs technologiques. Cette analyse pourra se décliner pour l'étude d'autres types de technologies, comme celles mentionnées dans les catégories 2, 3 et 4 de notre typologie.

ÉVITER DEUX ÉCUEILS : RÉDUCTIONNISME ET SOLUTIONNISME

En amont du choix d'un dispositif technologique, tout décideur doit avoir à l'esprit deux potentiels biais importants : le réductionnisme et son corollaire, le solutionnisme. Le **réductionnisme** consiste à « réduire » la réalité et l'ensemble des phénomènes à des équations mathématiques qu'il convient de calculer pour parvenir à une décision. Cette tendance est considérablement accentuée par le *big data*. En effet, le traitement algorithmique présente des avantages, mais comporte également le risque important de prendre la mesure (c.-à-d. la corrélation observée) pour la cause du phénomène (c.-à-d. la causalité de cette mesure). Concernant les applications de traçage, les mesures et les notifications (c.-à-d. les messages d'avertissement envoyés aux utilisateurs) ne sont pas explicables à l'utilisateur, car celui-ci n'obtiendra aucune information ni sur le lieu ni sur l'heure exacte du contact. L'utilisateur doit faire confiance à l'application sans pouvoir recueillir d'autres informations concernant les risques « réels », par exemple le pourcentage de risque d'infection associé qui serait à la fois un fonction du temps de contact, de la proximité, et d'éventuels autres facteurs.

L'étude menée des applications de traçage met en évidence le danger de s'en remettre automatiquement et sans sens critique à une mesure pouvant conduire à un **biais d'automatisation** (confiance inconditionnelle dans les résultats obtenus par l'application) ou à l'ostracisme envers autrui. Ainsi, ces dispositifs sont sur le point de devenir des proxy aux interactions sociales, car leur adoption conditionnera les rapports humains d'une manière positive (je suis testé négatif donc je peux avoir des interactions) ou négative (je suis à risque donc je suis ostracisé). Cette modification artificielle des rapports sociaux a donc le potentiel de renforcer ou au contraire d'affaiblir la confiance des individus non seulement dans leur concitoyens mais aussi dans le gouvernement, les institutions et les autorités publiques.

Sans tomber dans une critique trop simpliste de la technologie, il faut aussi se prémunir d'une forme de « **solutionnisme** » technologique qui voudrait résoudre, uniquement par des moyens techniques, des problèmes éminemment sociaux et politiques comme ceux posés par une situation de crise pandémique, relevant d'un enjeu de santé publique et touchant à la solidarité nationale et internationale. **La technologie peut ainsi devenir un alibi permettant aux décideurs de se dédouaner de l'absence d'autres initiatives.** À cela s'ajoute un enjeu connexe, celui de l'impératif technologique : c'est-à-dire, l'obligation morale de devoir recourir à une « solution » technologique sous prétexte qu'elle existe. Or, ce n'est pas parce qu'un outil technologique est accessible qu'il constitue nécessairement la réponse la plus appropriée (à savoir, la plus efficace, efficiente, socialement acceptable ou éthiquement responsable) au problème en question.

Ainsi, l'efficacité opérationnelle (Quelle est la qualité de la détection ? Quel est le taux de faux positifs ? etc.) et l'acceptabilité éthique d'une application numérique de lutte contre la COVID-19 ne peuvent jamais s'analyser isolément d'autres mesures sanitaires, ni des processus sociaux. L'expérience montre à ce sujet que les pays précurseurs du recours aux moyens numériques pour lutter contre la COVID-19, comme la Chine, Taïwan ou la Corée du Sud, ne retirent quelque efficacité de l'usage des technologies qu'en inscrivant soigneusement ce dernier au sein d'une politique de gouvernance beaucoup plus globale et multidimensionnelle de la crise. La participation sociale et politique des communautés et des corps intermédiaires, entre l'individu et l'État, permet un contrôle continu de l'efficacité de l'outil numérique et son adaptation aux besoins humains de la lutte contre la pandémie.

LE CHOIX DES TECHNOLOGIES ET DES DONNÉES COLLECTÉES

Un premier aspect concerne le **type de technologie** utilisée et le **type de données** qu'elle permet de collecter. Concernant les applications de suivi de porteurs de virus, on notera qu'elles permettent

d'identifier les personnes passées à proximité d'un individu signalant des symptômes, mais qu'elles ne peuvent pas identifier une possible contamination par un malade asymptomatique ou par une personne qui ne déclare pas son état à l'autorité médicale. La technologie représente une partie du dispositif, mais son efficacité dépend de facteurs humains.

Pour les applications de traçage, le choix du type de données collectées porte sur les données de localisation ou de proximité. Les premières permettent de suivre la position d'un individu et peuvent être collectées par des technologies **GPS** ; les secondes informent sur les interactions entre les personnes (contact ou passage à proximité…) susceptibles d'être des moments de contamination. Elles sont accessibles par le recours au Bluetooth.

Si les puces présentes dans les smartphones communiquant avec le réseau de satellites GPS donnent une position au mètre près, leur précision est mise à mal par les environnements urbains, surtout si l'utilisateur se trouve dans un grand bâtiment. Cela rend leur utilisation délicate dans des situations pourtant susceptibles de constituer des foyers de contamination. Le **Bluetooth** localise, quant à lui, un appareil par rapport aux autres

dispositifs connectés à proximité. Il fonctionne bien à l'intérieur des bâtiments. Cette technologie n'est cependant pas conçue pour évaluer les distances. La portée du signal dépend de la qualité de l'appareil, de sa position (tenu à la main, situé dans une poche ou un bagage) et de l'état de charge de la batterie. En outre, cette technologie ne permet pas d'établir de façon certaine qu'il y ait eu contact : le signal passe bien à travers une vitre (train ou voiture à l'arrêt, bâtiment...) et ne peut prendre en compte les contaminations par contact indirect, comme toucher un objet infecté, ou par des gouttelettes en suspension portées par le flux d'air d'un système de climatisation.

RISQUES TECHNIQUES ET ENJEUX DE SÉCURITÉ INFORMATIQUE DU BLUETOOTH

Parmi la dizaine d'initiatives étudiées dans le cadre du présent projet, la majorité repose sur l'utilisation de la technologie Bluetooth, voire des ***beacons***. Les appareils équipés de l'application se signalent entre eux grâce à l'envoi d'une courte information (16 octets), permettant à tout appareil de détecter un autre appareil qui se signale à proximité.

Ainsi, il est impossible pour un appareil d'envoyer un message qui ne serait compréhensible que par un nombre limité d'appareils autorisés, dès lors que l'algorithme d'exploitation de ces messages est public. Dans ces conditions, il est à la portée de tout individu ayant un minimum de compétences technologiques d'intercepter les signaux Bluetooth et même de diffuser des informations malveillantes grâce à son propre logiciel, ou en utilisant une version modifiée du logiciel d'origine. À titre d'exemple, l'amplitude de la portée d'un signal Bluetooth varie selon le matériel utilisé, une antenne spécialisée pouvant capter un tel signal jusqu'à plusieurs centaines de mètres en terrain dégagé. Or, il est impossible de limiter l'envoi d'une trame Bluetooth à 5 mètres maximum sur un smartphone, et il en va de même pour la réception.

Partant de ce constat, il existe toute un arsenal d'attaques plus ou moins préjudiciables qui peuvent être réalisées à l'encontre d'un dispositif de traçage. Un premier schéma d'attaque possible serait l'envoi d'une masse de fausses informations pour corrompre les données de l'application et la rendre inutile. Un attaquant disposant des capacités techniques pour intercepter et participer au dispositif à grande échelle pourrait aussi coupler les données collectées à d'autres informations (géolocalisation, indicateur de temps, prise de photos/vidéos), pour ré-identifier les utilisateurs qui se sont signalés positifs au COVID-19. Il est tout à fait possible d'extrapoler ensuite ces informations afin de les rattacher à des groupes d'individus ou communautés préalablement ciblés.

Ces attaques font peser un risque sur certaines des principales exigences des applications de traçage : la précision des données, le secret médical, l'anonymat, la confidentialité des rencontres (lieux, dates, identités). En ce sens, le projet DP-3T s'est montré particulièrement vigilant quant à l'ensemble de ces risques et améliore constamment son protocole pour les atténuer, voire les parer.

Dans le cas de la solution centralisée (par exemple, le projet de protocole ROBERT), le serveur est capable d'associer ces quelques octets à un identifiant d'appareil et une date précise. L'anonymat et la confidentialité des graphes de contacts sont des notions plus fragiles dans ce cas. Pour la solution décentralisée du protocole DP-3T, les quelques octets émis par un appareil représentent simplement une valeur aléatoire éphémère associée à une information de date grossière. Seul l'appareil émetteur serait capable d'identifier ses informations comme venant de lui-même. Il sera donc plus compliqué dans cette hypothèse de corrompre la confidentialité des informations. Avoir à l'esprit certains de ces éléments techniques permettra aux décideurs d'apprécier si les **risques** techniques et d'enjeux de sécurité informatiques qu'ils présentent **sont ou non résiduels**, afin d'aider dans le choix du dispositif technique à déployer.

CENTRALISATION VS DÉCENTRALISATION : UN CHOIX STRUCTURANT

Un aspect particulièrement structurant concerne le choix d'un système centralisé ou décentralisé. Centralisation et décentralisation sont souvent exposées en informatique comme une dichotomie nette. La réalité est, comme nous le verrons, plus fine et complexe.

Les deux systèmes sont viables d'un point de vue technique et présentent des avantages et désavantages sur le plan de la sécurité et de l'infrastructure. La principale différence n'est pas de nature technique, mais réside plutôt dans les

concepts que nous voulons intégrer dans ces systèmes en lien avec nos sociétés, nos droits et devoirs, les lois et l'éthique. La responsabilité et la protection de la vie privée sont les plus importants de ces concepts.

Par définition, les systèmes décentralisés (plus ou moins comme DP-3T ou COALITION) répartissent les rôles entre les différents acteurs participant au système. Dans un contexte décentralisé, la responsabilité devient une chaîne de responsabilité. En effet, un système décentralisé fonctionne si la chaîne de responsabilité est le fait d'un nombre suffisant d'acteurs légitimes dans le système (pas nécessairement la totalité d'entre eux). Ces systèmes sont fondés sur le concept plus général de « décentralisation », lequel renvoie aux concepts de participation au processus décisionnel, de représentation locale, de démocratie, d'égalité et de liberté. Pourtant, en raison du nombre accru d'acteurs responsables dans le système, la responsabilisation a un coût en raison des spécifications en amont, de la rigidité en aval et de la plus grande complexité des processus et systèmes de sécurité. Elle soulève également la question des utilisateurs malveillants qui envoient des données erronées, voire faussées, pour compromettre l'ensemble du système (l'incidence de ces utilisateurs peut être atténuée par des mécanismes d'autorisation associés à des autorités de certification plus ou moins centralisées). Elle soulève aussi la question de la gouvernance mondiale du système eu égard aux lois nationales et transfrontalières.

Un système centralisé (plus ou moins comme ROBERT) vise à regrouper la responsabilité au sein d'une entité centrale (le serveur central) qui assure l'uniformité et la cohérence de l'ensemble du système. Un tel système fonctionne parfaitement lorsqu'une seule entité a la capacité et l'obligation d'assumer toute la responsabilité (particulièrement dans le contexte d'organisations comme les États ou d'organisations regroupant plusieurs États comme l'UE). Il est beaucoup plus facile pour l'entité centrale de tout gérer : le niveau d'authentification et d'autorisation des utilisateurs, le cycle de vie des données (sécurité, authentification, certification) et l'évolution de l'infrastructure. Toutefois, cela sous-entend naturellement que cette entité centrale jouit de l'entière confiance des utilisateurs et n'utilise pas les données à mauvais escient (un « tiers de confiance »).

Parmi les risques liés à l'utilisation d'un tel système centralisé, notons :

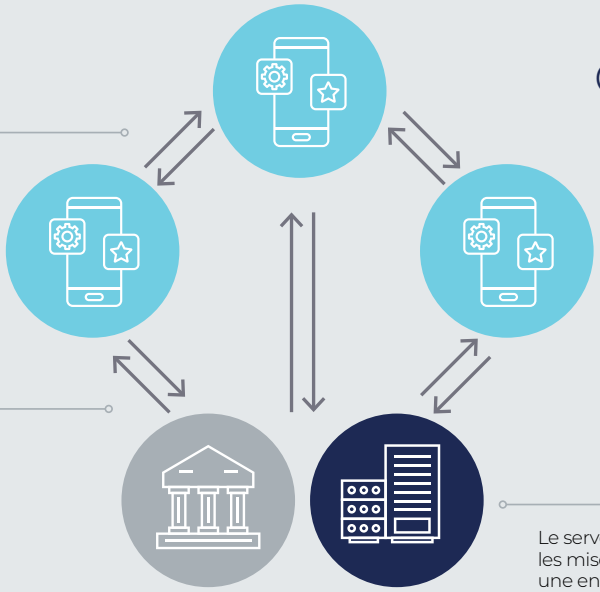
- **Point d'attaque unique :** La moindre brèche de sécurité dans un serveur exposerait l'ensemble du système fédéré et tous les utilisateurs des applications touchées. Une intrusion visant le serveur pourrait mener à l'identification des utilisateurs.

- **Établissement de liens avec les utilisateurs :** Avec un système centralisé, le serveur est capable d'apprendre les données de certains utilisateurs et d'établir des liens entre elles. Le serveur pourrait déduire que deux utilisateurs ont été en contact à un certain moment grâce aux données d'horodatage, ce qui lui permettrait d'établir un graphique social partiel reflétant ces contacts. De plus, le serveur pourrait utiliser les données de colocalisation pour établir l'identité de personnes ayant téléversé des données de manière anonyme en analysant la fréquence des téléversements et en faisant des recoupements avec les utilisateurs qui ont effectué les téléversements. En outre, le serveur pourrait utiliser les données sur la causalité pour établir l'identité de personnes ayant téléversé des données de manière anonyme puisque ces données sont préservées lors du téléchargement. Le serveur peut ainsi reconstituer une représentation graphique des pseudonymes en établissant une relation de causalité temporelle.

- **Traçage des utilisateurs :** Le serveur centralisé crée des identifiants éphémères et peut, à un certain point, lier les identifiants éphémères passés et futurs d'un utilisateur donné, infecté ou non, en décryptant son identifiant permanent. Le serveur, en combinant ces données à d'autres ensembles de données, comme celles de télévisions en circuit fermé, peut suivre toutes les personnes, infectées ou non. Compte tenu d'un identifiant éphémère cible, comme celui d'une personne suspecte recueilli par les représentants de la loi, il est possible d'étiqueter et de classer les personnes de telle sorte que des tiers peuvent les reconnaître sans avoir accès au serveur ou à la base de données centralisés. Par exemple, les identifiants éphémères de ROBERT ne sont pas authentifiés, et le serveur ne fournit aucune preuve que l'identifiant est chiffré ou que la bonne clé a été utilisée. Cette capacité pourrait permettre à des représentants de la loi, ou d'autres acteurs, sans

SYSTÈME CENTRALISÉ

Seule l'information brouillée (*obfuscation*) est échangée entre les appareils physiquement à proximité. L'information privée ne quitte jamais l'appareil dans ces échanges.

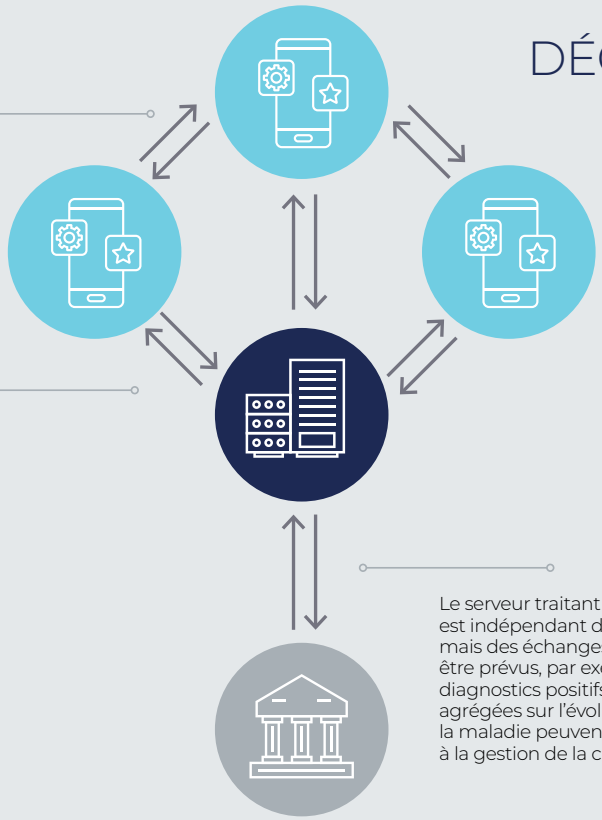


L'information à jour est transmise à un serveur central qui traite et distribue les mises à jour à travers le réseau des utilisateurs. À la différence du modèle décentralisé, ici les échanges contiennent des informations clés au traçage des contacts. La sécurité des informations est assurée à travers plusieurs protocoles de cryptage et anonymisation.

Le serveur traitant et distribuant les mises à jour est géré par une entité administrative. Ceci permet d'exploiter un maximum d'informations provenant du traçage des contacts au profit d'une stratégie centralisée de gestion de crise sanitaire.

SYSTÈME DÉCENTRALISÉ

Seule l'information brouillée (*obfuscation*) est échangée entre les appareils physiquement à proximité. L'information privée ne quitte jamais l'appareil.



L'information à jour est transmise à un serveur central qui traite et distribue les mises à jour à travers le réseau des utiisateurs. L'information échangée n'est pas utile en soi. Seule l'application de chaque appareil peut transformer ces mises à jour en information utile pour les utilisateurs.

Le serveur traitant et distribuant les mises à jour est indépendant des entités administratives, mais des échanges des mises à jour peuvent être prévus, par exemple, dans la collecte des diagnostics positifs. Quelques informations agrégées sur l'évolution de la transmission de la maladie peuvent être produites pour aider à la gestion de la crise sanitaire.

accès à la base de données dorsale, de retracer des mouvements d'utilisateurs et de collectivités précis en leur attribuant des identifiants distincts et en reconnaissant leurs émissions Bluetooth, ce qui pourrait entraîner le traçage à long terme de personnes ou de membres des collectivités (étant donné qu'il est possible d'attribuer des identifiants précis à des groupes cibles de personnes) par des tiers.

- **Note :** Ces attaques hypothétiques représentent un risque et dépendront des mesures d'atténuation mises en œuvre dans la solution au moment de sa production. Il existe des façons de réduire le risque, comme l'indiquent les spécifications du DP3T.

Les limites des systèmes tant centralisés que décentralisés peuvent être assouplies pour atténuer leurs inconvénients respectifs, ce qui ouvre la voie à de nouveaux types d'attaques :

- Exemple 1 : Le protocole ROBERT est conçu pour déléguer la collecte et le brouillage de données aux utilisateurs, mais des clés sont générées par le serveur central. Il ouvre la porte à des attaques possibles par des utilisateurs malveillants qui saisissent de mauvaises données. Il n'est en revanche pas clair si, dans l'application StopCovid afférente, une étape de validation par une autorité est ajoutée, en raison du code QR qui existe entre la santé publique et l'application.
- Exemple 2 : Dans les systèmes décentralisés, les utilisateurs doivent s'authentifier et se soumettre à un processus de certification pour atténuer le risque lié aux utilisateurs malveillants. Mais une autorité d'authentification est un système plus centralisé, ce qui pose problème sur le plan de la confiance.

Ainsi, **l'apparente dichotomie** opposant centralisation et décentralisation est **en réalité plus fine** que cela, certains éléments d'une solution pouvant être décentralisés alors que d'autres non. Si bien que la plupart des dispositifs technologiques apparaissent en réalité **hybrides**, par un choix de composants à la fois centralisés et décentralisés.

Plusieurs conséquences en découlent, comme il sera présenté dans l'encadré ci-dessous. Par exemple, des systèmes comme DP3T/Coalition sont en partie décentralisés : la collecte, l'échange et la vérification des données sur les contacts sont décentralisés du côté client ; les personnes sont responsables de leurs propres données. Mais le stockage des données sur les personnes infectées continue d'être centralisé dans le serveur central. Nous pourrions imaginer de pousser plus loin la décentralisation en décentralisant le stockage.

Comparaison uniquement fondée sur des aspects de la (dé)centralisation et des caractéristiques de haut niveau pour lesquels il existe des différences importantes.

Catégories	ROBERT	DP-3T	Coalition	Google/Apple	MILA
Traçage par Bluetooth	Oui	Oui	Oui	Oui	Oui
Traçage par GPS	Non	Non	Oui (pour la localisation approximative)	Non	Oui
Collecte de données sur les contacts	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Chiffrement des données sur les contacts	Décentralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Production des clés secrètes des contacts	Centralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Stockage des données sur les contacts	Centralisé	Centralisé	Centralisé	s. o.	Centralisé
Évaluation du risque d'infection	Centralisé	Décentralisé	Décentralisé	Décentralisé	Décentralisé
Échange des données sur les contacts lorsqu'ils sont déclarés positifs	Envoi des clés des autres contacts	Envoi des clés des autres contacts	Envoi des clés des autres contacts	Envoi de ses propres clés de contacts	Envoi de ses propres clés de contacts Envoi de la localisation brouillée
Échange des données sur les contacts au moment de l'évaluation du risque d'infection	Envoi de ses propres clés de contacts	Téléchargement des clés des contacts des utilisateurs infectés	Téléchargement des clés des contacts des utilisateurs infectés	s. o.	Téléchargement des clés des contacts des utilisateurs infectés
Collecte des données des utilisateurs privés	Non	Non	Localisation approximative	Non	Oui
Système prédictif	Non	Non	Non	Non	Oui
Système potentiellement transfrontalier	Oui	Oui	Oui	s. o.	Non
Utilisation possible à d'autres fins que le traçage de contacts	Non	Non	Non	Non	Oui
Authentification humaine requise lorsqu'une personne est déclarée positive	Possiblement	Possiblement	Non	s. o.	Oui
Complexité relative de l'infrastructure du serveur (1 : de base à 5 : complexe)	2	3	3	s. o.	5
Open source	Partiellement en source ouverte (protocole + modèle de données)	Oui (kit de développement de logiciels pour appareils mobiles et serveurs)	Oui (*mobile library*)	À déterminer	À déterminer
Organisation	Gouvernemental	À but non lucratif	À but non lucratif	À déterminer	À but non lucratif

s. o. : sans objet

RECOMMANDATIONS

Il est possible d'avoir recours à des technologies efficaces sans pour autant sacrifier nos libertés individuelles et droits fondamentaux. Un choix éclairé des dispositifs technologiques nécessite d'en connaître les caractéristiques techniques sous-jacentes.

Cette connaissance des aspects techniques devra profiter - par un nécessaire **travail de pédagogie** - à l'ensemble d'une organisation ou d'une société, afin de faciliter son adhésion. Par exemple, pour limiter toute fracture numérique, il conviendra d'être inclusif et didactique (Vos salariés savent-ils ce qu'est le Bluetooth, comment fonctionne une blockchain, où sont stockées les données ? Comptez-vous communiquer sur le possible pourcentage de faux positifs de votre dispositif ? etc.). Gouvernements comme entreprises devront veiller à ne pas accentuer les conséquences de l'inégalité d'accès aux dispositifs technologiques, sous peine de pénaliser ceux qui sont déjà largement exclus du numérique. En outre, les informations fournies aux utilisateurs doivent faire ressortir très clairement le fait qu'aucune application ne saurait être considérée comme un dispositif médical, malgré les notifications et recommandations, et ne remplace pas un test de dépistage.

Les comparaisons établies au titre de l'analyse des applications de traçage permettent d'illustrer les questions à se poser. Ces enjeux se déclinent également en cas de déploiement d'autres types de technologies (objet connecté, caméra thermique, système d'IA, blockchain, etc.), en prenant soin d'adapter l'analyse en fonction des spécificités de chaque projet envisagé.

Dans ces circonstances, tout décideur se doit de développer un **regard critique** face à ces choix de dispositifs technologiques. Par exemple, lorsque le code de l'outil envisagé n'a pas été contrôlé par des tiers indépendants, il n'existe aucune garantie que les données soient effectivement traitées de la manière spécifiée par le porteur du projet. C'est pourquoi nous recommandons de prévoir soit l'existence d'un organe de contrôle indépendant, ce qui paraît surtout approprié dans le cadre d'un dispositif gouvernemental, soit de prévoir l'auditabilité par un tiers, particulièrement propice dans le cadre de l'entreprise. Une autre recommandation à cet égard serait d'obliger ces prestataires à conduire des mesures d'impacts (comme celle figurant à l'Annexe n° 2) qui soient distinctes et accessibles au public.

Les mesures techniques ne suffiront certainement pas à garantir en soi la protection des individus. Tout gouvernement doit être conscient de l'importance du **contexte législatif, social et politique** dans lequel de tels dispositifs pourraient être déployés. Ainsi, il conviendra si nécessaire d'adopter des dispositions légales et réglementaires visant à assurer la protection des libertés individuelles et des droits fondamentaux ainsi que d'éviter la discrimination ou la stigmatisation de certains groupes.

Enfin, au-delà ou en complément des objectifs immédiats visés par l'utilité d'une technologie, tout décideur devra prendre en compte les besoins de la **transition écologique** dans l'outil technologique privilégié. La crise sanitaire ne doit pas éclipser la crise climatique auquel l'humanité et tout un chacun est exposée.

CHAPITRE 3

DÉFINIR UN MODÈLE DE GOUVERNANCE

En fondant notre compréhension de la situation sur le référentiel approprié et fort d'une connaissance détaillée des différentes technologies disponibles, il est possible de bâtir une stratégie employant des dispositifs technologiques pour combattre la pandémie, relancer une activité économique ou, plus généralement, agir dans le contexte issu de la crise.

Pour faire les choix les plus appropriés et assurer un accueil positif du projet, **la clé du succès nous semble résider dans la gouvernance**. La méthode détaillée dans le présent chapitre pourra inspirer les décideurs dans l'élaboration de leur stratégie et notamment dans les modes de sélection, de déploiement et de pilotage de dispositifs technologiques.

Cette méthode se fonde **sur six principes, guidant l'ensemble de la démarche et sur un mode de gouvernance participatif**. En effet, le contexte de crise actuel nécessite d'avoir recours à des solutions novatrices et d'obtenir une acceptation sociale réelle, deux éléments que l'intégration de toutes les parties prenantes dès le début du processus décisionnel aidera à obtenir. La présence de **compétences techniques, juridiques et éthiques** au sein de l'organe de gouvernance nous semble également déterminante.

Lors de l'étape méthodologique de validation du choix d'une technologie, ces six principes prendront la forme de **critères concrets réunis dans une grille d'évaluation**. Rempli par l'instance de gouvernance participative du projet, ce document permettra d'aborder tous les aspects de la technologie étudiée et constituera une base de discussion pour le processus décisionnel. Il pourra servir de fil conducteur tout au long d'un projet géré en mode agile, afin de s'assurer que les mesures prises sont cohérentes avec les évolutions de la situation sanitaire et économique.

Cette méthode peut être employée par tout type d'institution. Des **recommandations spécifiques à son déploiement en entreprise** sont rassemblées dans les encadrés en fin de partie.

Notre rapport a pu rappeler à quel point il est essentiel de déterminer le référentiel adéquat pour envisager cette crise protéiforme, notamment sanitaire et socioéconomique (**cf. Partie I**). La compréhension des caractéristiques des technologies se révèle tout aussi fondamentale pour connaître leur influence sur nos libertés individuelles et collectives, ainsi que sur la conduite de nos sociétés (**cf. Partie II**). Il s'agit désormais de déterminer comment définir un modèle de gouvernance des dispositifs technologiques envisagés. En effet, la SARS-COV2 a et aura un impact sans précédent sur le fonctionnement de nos organisations, en particulier pour les entreprises. Dans ces circonstances, il convient de fonder la gouvernance sur des principes clés. Nous proposons dans cette dernière partie du rapport une analyse sur deux niveaux : d'une part, en identifiant des valeurs éthiques et des normes juridiques et d'autre part, en les reliant à différents critères déployés au sein d'une grille d'analyse d'impact multi-facteurs. Cette analyse d'impact - qui se veut un outil de bonne gouvernance pour le déploiement responsable de technologies COVI et dont un mode d'emploi est détaillé ci-après - permet ainsi de dépasser la simple appréciation de la protection des données ou la réductrice opposition entre vie la privée des individus et sécurité publique, pour proposer une méthode concrète de sélection, de déploiement de solutions de sortie de crise. Nous aborderons ainsi dans cette troisième partie la nécessité d'une gouvernance inclusive et participative pour éviter tout délitement du lien social, et en particulier ses modalités de déploiement au sein des entreprises.

MODE D'EMPLOI DE LA MÉTHODE DE SÉLECTION, DE DÉPLOIEMENT ET DE GOUVERNANCE DE STRATÉGIE DE GESTION DE CRISE SANITAIRE FONDÉE SUR DES DISPOSITIFS TECHNOLOGIQUES

La nature spécifique du risque pandémique implique que le redéploiement de l'activité économique et sociale passe par le développement, au sein des organisations, d'une **forme d'immunité et de résilience collective**. Cette démarche requiert l'adhésion active et la responsabilité de chacun, au sein d'une culture éthique de l'utilisation des technologies. Elle nécessite donc une approche participative, permettant de contextualiser les choix technologiques et de prendre en compte la diversité des situations concrètes rencontrées par les différents acteurs et les enjeux éthiques auxquels ils font face. En outre, l'inextricable lien entre la dimension technique, juridique et éthique nous oblige à aborder la question du déploiement de dispositifs technologiques de manière **systémique**. Nous proposons donc une méthode d'**analyse multi-facteurs**, qui doit être mise en œuvre par une équipe **multidisciplinaire**.

Une telle analyse commence par étudier **les objectifs** qu'un dispositif technologique doit atteindre, à travers sa finalité, le contexte dans lequel il est développé ou encore l'écosystème dans lequel il s'intègre : son efficacité doit être appréciée au regard de l'ensemble de la stratégie à laquelle son déploiement prend part.

Cette démarche conduit ensuite à interroger **les caractéristiques techniques** des dispositifs envisagés. Ainsi, à titre d'exemple, une application reposant sur un protocole centralisé ou décentralisé implique des choix de gouvernance structurants. De même, les questions d'interdépendance et d'interopérabilité avec d'autres technologies externes paraissent cruciales.

Par ailleurs, il convient d'adresser les défis liés à l'**acceptabilité sociale**. Les risques de détournement ou de mésusage de la solution doivent être pris en compte, de même que d'autres risques sociaux, comme le creusement de la fracture numérique ou les formes de discrimination.

La question de la **temporalité** est également au cœur du sujet : un dispositif technologique nécessaire pour aider à la sortie de crise peut finir par se révéler disproportionné. Il convient de déterminer les critères qui caractérisent une « situation de crise » au sein de l'organisation. L'utilisation d'une telle solution doit-elle se prolonger tant que des foyers épidémiques sont identifiés dans le monde, ou si la maladie prend la forme d'une épidémie saisonnière ? Faut-il adopter une logique de prévention d'une nouvelle épidémie ?

De façon concrète, pour mettre en œuvre la méthode ici proposée, **la première étape consiste à constituer un organe de gouvernance approprié**, impliquant des représentants de l'ensemble des parties prenantes et doté de compétences techniques, juridiques et éthiques. Cet organe est destiné à accompagner le projet depuis sa conception jusqu'à son arrêt.

Dans un premier temps, nous recommandons que le groupe ainsi constitué prenne connaissance des principes et des éléments de contexte décrits dans le présent rapport, susceptibles de constituer un **référentiel commun**.

Cette instance sera alors à même de qualifier le besoin, en regard des nécessités de l'organisation, mais également en fonction des **réalités du terrain** telles que les pratiques professionnelles, les habitudes et les inquiétudes, décelées à la lumière de la connaissance des utilisateurs. Cette démarche permet d'identifier les contraintes mais aussi des éléments de solutions efficaces proposés par les acteurs de terrain. Lors de cette phase, il sera important de rester focalisés sur **l'expression des besoins**, perçus du point de vue des utilisateurs, et de ne pas aborder trop rapidement les solutions technologiques. Il conviendra aussi de concevoir une réponse globale à la situation donnée, dans laquelle les outils technologiques viendront s'insérer.

Une fois les besoins de l'organisation identifiés, **la typologie de technologies** disponibles et les exemples présentés dans les sections précédent pourront guider le choix à opérer.

Quand un processus est esquissé et une solution technologique choisie, **la grille d'analyse** figurant en Annexe n° 2 permet de **faciliter la validation de ces décisions**. Il convient de noter que cet outil, conçu pour les besoins de notre démarche avec des membres de l'association ITechLaw et des collaborateurs de la Human Technology Foundation, n'est pas seulement destiné à évaluer les risques juridiques liés à la mise en œuvre d'un projet, mais aussi à renforcer les pratiques de bonne gouvernance et à servir de soutien à des décisions efficaces, prises dans le cadre d'une démarche éthique. Son objectif est d'inciter l'ensemble des décideurs à **se poser les bonnes questions dès le début du projet** et de fournir une vision à la fois très large et détaillée du dispositif technologique examiné. Le processus se déroule en sept étapes, correspondant aux valeurs éthiques exposées ci-après. Chaque étape rassemble des questions permettant d'évaluer la pertinence du dispositif proposé au regard de l'impératif de satisfaction de l'intérêt général, mais aussi de la situation des utilisateurs.

Plus l'instance de gouvernance utilisant cette grille est **inclusive**, plus cette photographie prendra en compte la diversité des aspects du dispositif étudié. Elle constituera ainsi un outil d'objectivation et un support de discussion commun à des interlocuteurs venant d'horizons différents.

La grille d'analyse proposée est volontairement très détaillée, afin de répondre aux besoins des grandes organisations mettant en œuvre des projets complexes. Elle peut cependant être utilisée de façon simplifiée, en ayant soin de respecter les sept étapes du cheminement :

1. Objectifs éthiques et avantages pour la société (*Ethical Purposes and Societal Benefit*)
2. Responsabilité (*Accountability*)
3. Transparence et explicabilité (*Transparence and Explainability*)
4. Equité et non-discrimination (*Fairness and Non-Discrimination*)
5. Sécurité et fiabilité (*Safety and Reliability*)
6. Open data et propriété intellectuelle (*Open Data, Fair Competition and Intellectual Property*)
7. Données personnelles et vie privée (*Privacy*)

Les deux premières colonnes de cette grille permettent de décrire la technologie étudiée, ainsi que les enjeux éthiques ou les risques qu'elle peut présenter. Nous conseillons de les remplir en premier, pour permettre une évaluation par les membres de l'instance de gouvernance. En effet, la mise en œuvre d'une solution technologique implique toujours de faire des **arbitrages** et de **prioriser** les principes que l'on souhaite voir respectés. Cette démarche conduit à établir un cadre de règles communes. Il pourra comporter des contraintes ou des restrictions, qui doivent être acceptées et intériorisées pour être **efficacement appliquées sur la durée**.

Si, au cours de cette démarche, des points considérés comme bloquants subsistent, la colonne « mesure d'atténuation » permet d'étudier des moyens de rendre ces contraintes acceptables pour tous et ainsi de lever les difficultés par le dialogue. La démarche peut être réalisée pour plusieurs dispositifs envisagés, la comparaison des colonnes « enjeux et risques » permettant de les départager et de choisir le plus adéquat.

Une fois la décision prise de déployer une solution fondée sur un dispositif technologique, cette grille d'analyse pourra être utilisée à chaque itération d'un processus agile, afin d'assurer un suivi des points d'attention. Elle pourra aussi fournir les éléments clés de la communication permettant une large adoption de ce dispositif par ses utilisateurs.

Pour un déploiement en entreprise, on pourra se reporter aux spécificités décrites dans l'encadré ci-après.

FONDER LA GOUVERNANCE SUR DES PRINCIPES CLÉS

Les choix des États comme des entreprises ou de toute organisation, en matière d'applications de traçage liées au COVID-19, ne sont pas anodins et relèvent de choix et d'orientations tant en termes de gouvernance des technologies que de gouvernance de la crise sanitaire elle-même. Ainsi, un regard éthique qui met en lumière les valeurs ou principes privilégiés (de façon volontaire et explicite ou non) et leurs implications quant à la façon dont sont conçues, déployées et mises en œuvre ces applications, peut nous fournir un éclairage utile devant les difficiles choix que les entrepreneurs et décideurs publics ont à faire en ces temps de crise et souvent en urgence.

Le modèle de gouvernance collective de la crise que nous appelons ici, repose sur un socle de valeurs qui nous semblent pertinentes pour une analyse des diverses solutions technologiques et plus particulièrement celles fondées sur le traçage.

Chacune des six valeurs éthiques présentées ci-après trouvent une déclinaison pratique dans les critères de notre grille multifactorielle ainsi que le tutoriel d'emploi ci-dessus vient de l'exposer.

En se basant principalement sur des documents publics, des membres de l'association ITechLaw et des collaborateurs de la Human Technology Foundation ont appliqué la grille d'impact multifactorielle (v. Annexe n° 2) à l'ensemble des 11 technologies sous étude : DP3T, TraceTogether, COVI App, ROBERT, Apple/Google API, Aarogya Setu, COALITION, NHSx, Corona-Datenspende, TerraHub et Estimote. Ensuite, nous avons produit un document de synthèse des constats clés (*key findings*) remarqués par les équipes en appliquant la grille. Nous reproduisons trois exemples de nos synthèses des constats clés en Annexe n° 4. En Annexe n° 3, nous fournissons un tableau comparatif des 11 technologies.

Ci-dessous, nous avons ainsi choisi de présenter chaque principe au vu d'un **double niveau d'analyse** : en premier lieu nous avons présenté le concept juridico-éthique de base ; et, ensuite en encadré, nous avons présenté des déclinaisons opérationnelles de chaque principe par des illustrations issues de nos grilles d'impact multifactorielles des 11 technologies (que celles-ci paraissent positives ou non).

1. LA PLUS-VALUE EST SANS DOUTE LE PREMIER CRITÈRE À PRENDRE EN CONSIDÉRATION, encore que la compréhension du terme renvoie à diverses conceptions du bénéfice attendu du système technologique. Il importe de ne pas privilégier outre mesure l'un ou l'autre point de vue, du moins dans un premier temps, mais d'envisager la pluralité de ceux-ci avant toute décision. La plus-value se mesure, d'abord, en termes de santé publique et suppose la comparaison de diverses méthodes technologiques mais également non technologiques. Il s'agit alors de considérer l'apport de chacune d'elles ou de leur combinaison à la lutte contre de nouvelles contaminations. Cette plus-value s'apprécie aussi en termes économiques lorsqu'il s'agit des coûts liés directement ou indirectement à la mise en place et au fonctionnement du *contact tracing*, mais également lorsqu'on calcule l'impact sur l'activité économique de la persistance de la pandémie. Elle s'évalue également en termes de bien-être psychologique de la population. Cette valeur trouve sa déclinaison dans le critère n° 1 de la grille multifactorielle (Annexe n° 2), dont certaines illustrations sont étudiées dans l'encadré qui suit.

OBJECTIFS ÉTHIQUES ET AVANTAGES POUR LA SOCIÉTÉ

Corona-Datenspende se traduit littéralement en français par « don de données sur le coronavirus », ce qui reflète bien en quoi consiste cette application : elle encourage les citoyens allemands à fournir, sur une base volontaire, des données à leur sujet provenant de moniteurs d'activité ou d'applications sur la santé. Elle ne vise pas à fournir une rétroaction directe sur leur état de santé personnel, mais uniquement à appuyer les travaux de chercheurs pour le bien-être de la société. Au chapitre des objectifs éthiques et des avantages pour la société, cette application, ou du moins l'idée qui sous-tend son déploiement, se démarque : selon les résultats obtenus par une étude reposant sur les données recueillies au moyen de « Corona-Datenspende », ou du moins les utilisant, l'application pourrait contribuer à renforcer chez les gens l'impression que chaque personne compte et que chacun peut faire sa part pour ralentir la pandémie. Au sens plus large, le débat public qui s'est engagé sur le don de données personnelles pourrait également renforcer chez les gens la perception selon laquelle leurs données ont une valeur pour les chercheurs, mais aussi pour toute instance gouvernementale ou entité privée cherchant à s'en approprier, et que la décision de les « donner » doit être mûrement réfléchie.

L'**application NHSx** du Royaume-Uni, laquelle fait actuellement l'objet d'un test bêta réalisé sur l'île de Wight (petite île au large du littoral sud de l'Angleterre faisant partie des îles Britanniques), repose sur l'autodiagnostic (confirmé ou non) de l'utilisateur. Cette application utilise les informations sur les rencontres de proximité (les codes d'identification transmis, c.-à-d. les codes d'identification de sonar cryptés ainsi que les informations sur l'heure de la rencontre et la puissance du signal radio) téléversées par les utilisateurs, soit lorsqu'ils a) se sont autodiagnostiqués comme étant infectés (en fonction des symptômes qu'ils ont indiqués aux fins d'évaluation par l'outil) OU b) déclarent avoir reçu une confirmation de résultat positif à un test de dépistage du virus. Les informations fournies devraient indiquer au serveur sonar de traitement centralisé les appareils qui se sont trouvés dans une proximité immédiate les uns des autres ainsi que la durée et la distance de cette proximité. Le Royaume-Uni hésite encore à choisir une application centralisée ou décentralisée. S'ajoute à cela le fait que les autorités britanniques ont récemment demandé la mise en œuvre d'une fonction de traçage de contacts manuelle avant de finaliser l'application (alors que cela avait toujours été perçu comme une activité complémentaire). Dans ce cas, il est probable que cela réduise l'efficacité de l'application, quel que soit son mode de déploiement, et, par conséquent, que ses objectifs éthiques et ses avantages pour la société seront mis en doute.

L'**application COVI Canada** (« COVI ») est une application mobile décentralisée de traçage de contacts et d'évaluation du risque qui a été développée par un consortium dirigé par l'Institut québécois d'intelligence artificielle (« MILA »). L'application est conçue pour le traçage des contacts entre les utilisateurs, de façon à évaluer leur risque d'infection par la COVID-19 et à leur fournir des recommandations sur leur comportement actuel ou à la suite de changements du niveau de risque. Elle vise également à fournir aux autorités gouvernementales des informations agrégées sur les risques de contagion afin de les aider à concevoir des réponses plus efficaces à la pandémie. À l'instar d'autres applications de traçage de contacts, on estime qu'il faudra un taux d'adoption de 60 % de l'application COVI dans la population pour assurer l'efficacité et la précision de l'aspect IA (données agrégées, modèles épidémiologiques, etc.). Or, en raison des caractéristiques améliorées par l'IA propres à l'application COVI (données agrégées, modèles épidémiologiques, etc.), MILA estime que le pourcentage minimal requis est beaucoup plus bas, soit environ 10 %. Par conséquent, l'application devrait théoriquement apporter un avantage à la société, même si le taux d'adoption au sein de la population n'atteint pas le seuil de 60 % requis par la plupart des applications de traçage de contacts.

2. LA TRANSPARENCE EST LA CONDITION MÊME DU DÉBAT ÉTHIQUE. Comment pouvons-nous discuter de ce qui serait bien et bon si nous ignorons les tenants et les enjeux de nos discussions ? En l'occurrence, il s'agit d'éclairer le citoyen, tout citoyen, sur les enjeux d'un débat qui est certes technique mais surtout et en définitive politique, au sens de conduite de la cité. Quelles solutions technologiques ? Quelles options de rechange ? Quels acteurs derrière chaque solution ? Qui gère le système, avec quelles données et comment ? Ainsi, quand on parle de solution Bluetooth, il importe de savoir pour quelle population cette solution convient ou plutôt quelle population en sera exclue ? Avec quels risques d'erreurs ? Les efforts de certains organismes de recherche de décrire en *open access* les particularités de son système technologique sont louables. C'est un devoir de l'État ou plutôt d'une commission indépendante d'experts de diverses disciplines de fournir cette information (en format vulgarisé et accessible), non pour décider mais pour répondre aux demandes de tous bords et de permettre un vrai débat d'idées de la part de toute la population. Cette valeur trouve sa déclinaison dans le critère n° 3 de la grille multifactorielle (Annexe n° 2), dont certaines illustrations sont étudiées dans l'encadré ci-après.

TRANSPARENCE ET EXPLICABILITÉ

Les résultats de notre analyse indiquent que l'**application COVI** se distingue au chapitre de la transparence et de l'explicabilité. Tout d'abord, pour veiller à ce que les utilisateurs comprennent bien les éléments clés des conditions générales et qu'ils ne se contentent pas de les accepter sans les lire, une approche « progressive » à plusieurs niveaux sera adoptée. Par exemple, une couche supérieure graphique illustrant les implications en matière de vie privée peut être reliée à une deuxième couche un peu plus textuelle — celle-ci peut alors renvoyer à la section plus longue de la FAQ sur le site Web qui, à son tour, renvoie les utilisateurs à la politique complète de protection de la vie privée. Deuxièmement, selon le livre blanc sur l'application COVI, on s'assure que les utilisateurs ont bien compris plutôt que de le tenir pour acquis : « *[MILA] applique l'analyse dans l'application pour estimer la compréhension des utilisateurs — par exemple, en examinant le temps moyen que chaque utilisateur a passé à regarder les différentes couches d'informations divulguées. Ensuite, nous procédons à des questionnaires de compréhension dynamiques pour un échantillon aléatoire d'utilisateurs, ce qui nous permet de comprendre quelles informations ont été ou non internalisées. Enfin, les outils de divulgation sont révisés régulièrement en fonction des commentaires sur ces mesures, afin de s'assurer qu'ils répondent au mieux au comportement réel des utilisateurs.* » Troisièmement, les données de sortie du modèle peuvent être expliquées et les décisions, vérifiées. L'utilisateur ne reçoit pas d'informations spécifiques sur le calcul de l'évaluation des risques. Il ne recevra que des recommandations et des conseils personnalisés qui seront mis à jour au fur et à mesure que de nouvelles informations seront disponibles. Quatrièmement, MILA mettra en place une page Web pour l'application (où les utilisateurs pourront trouver la politique de protection de la vie privée), qui expliquera comment soumettre une plainte à propos du traitement des informations personnelles relativement à l'application.

L'application Aarogya Setu est une application mobile mise au point par le gouvernement indien en partenariat avec le secteur privé et visant à fournir des informations sur la santé et à assurer le traçage des contacts grâce aux données Bluetooth et de localisation GPS des utilisateurs. En réponse aux pressions des citoyens, des chercheurs et de groupes de la société civile, le gouvernement a récemment modifié sa position sur deux caractéristiques controversées de l'application. La première tient au manque de transparence lié au fait que le code source de l'application ne soit pas ouvert. Dans le passé, des reportages dans les médias ont fait état de tests d'intrusion révélant les problèmes de sécurité de l'application, qui ont été contestés par ses concepteurs. Toutefois, il est difficile de se prononcer sur la véracité des prétentions formulées de part et d'autre tant que le code source de l'application n'aura pas été vérifié par un groupe de chercheurs indépendants. Le gouvernement a depuis entamé un processus visant à corriger cette lacune, à commencer par la publication du code côté client de l'application pour la plateforme Android et le lancement d'un programme de prime aux bogues pour encourager l'apport d'améliorations au code. Il a également annoncé que le code de la version iOS et celui du serveur seraient ensuite rendus publics. De plus, les conditions d'utilisation de l'application ont été modifiées afin d'en retirer l'interdiction de soumettre l'application à la rétro-ingénierie. L'accès à l'intégralité du code est nécessaire afin de permettre à des tiers indépendants d'en effectuer la vérification et d'évaluer si les données sont effectivement traitées de la manière exacte indiquée par le gouvernement.

3. LA VALEUR D'AUTONOMIE ET LE RESPECT DES CHOIX PERSONNELS SONT À AFFIRMER. Cette valeur éthique, incarnée en droit par le concept de *privacy*, ne peut signifier la revendication individualiste d'un choix égoïste mais plutôt la réclamation d'une capacité de développement personnel. Une société démocratique se doit de garantir cette capacité dans la mesure même où ce développement constitue une garantie de pleine participation de chacun à la vie démocratique. Cette conception de l'autonomie interdit donc d'opposer intérêt individuel et intérêt collectif ; elle les envisage comme renvoyant l'un à l'autre, en relation dynamique. L'autonomie fonde la responsabilité de chacun par rapport à l'obtention du bien commun. On ajoute que cette recherche du bien commun ne peut s'arrêter aux frontières nationales, mais prend en compte la solidarité globale qu'impose la maladie. Cette valeur trouve sa déclinaison dans le critère n° 7 de la grille multifactorielle.

DONNÉES PERSONNELLES ET VIE PRIVÉE

L'« API de traçage de contacts d'Apple/Google », appelée « **API d'Apple/Google** », est une solution complète qui comprend des interfaces de programmation d'applications (API) et une technologie au niveau du système d'exploitation pour permettre le traçage de contacts. Pour assurer la protection de la vie privée, ce protocole s'appuie sur un nouveau concept : des identifiants pseudoaléatoires Bluetooth, appelés identifiants de proximité permanents. Chaque identifiant de proximité permanent provient d'une clé d'identifiant de proximité permanent, qui, elle, provient d'une clé d'exposition temporaire et d'une représentation du temps discrétisée. L'identifiant de proximité permanent change au même rythme que l'adresse aléatoire Bluetooth, pour empêcher la liaison et le traçage sans fil. Les métadonnées cryptées connexes identifiant un non-utilisateur sont liées aux identifiants de proximité permanents. Les métadonnées d'un utilisateur transmises ne peuvent être décryptées que lorsque l'utilisateur est déclaré positif.

À l'origine, le protocole **ROBERT** (*ROBust and privacy-presERving proximity Tracing*) était une proposition pour l'initiative de traçage de proximité paneuropéen (*Pan European Privacy-Preserving Proximity Tracing* (PEPP-PT), dont le principal objectif est de permettre le développement de solutions de traçage de contacts qui respectent les normes européennes de protection des données, personnelles et de sécurité, dans le cadre d'une réponse mondiale à la pandémie. Il a été noté que, pour le moment, l'application « StopCOVID », appuyée par le gouvernement français, semble être la seule application conçue selon le protocole ROBERT. De nombreux autres pays qui disaient appuyer le PEPP-PT semblent être passés au DP3T, en utilisant une structure décentralisée plutôt que l'approche centralisée ROBERT. Certains développeurs initiaux du PEPP-PT ont également annoncé avoir abandonné le projet en raison de préoccupations sur la centralisation, la transparence et la protection de la vie privée.

Quant au dispositif portable **Estimote**, il émet et effectue des balayages à la recherche d'autres appareils portables. Si le système détecte que deux appareils portables (ou plus) sont trop près l'un de l'autre, c'est-à-dire qu'ils ne respectent pas les directives de distanciation physique, les employés sont avertis par leur appareil portable, grâce à une lumière clignotante et à un signal sonore qui augmente en intensité et en fréquence à mesure que les employés se rapprochent l'un de l'autre. Estimote n'a pas mis à jour ses modalités d'utilisation ou sa politique sur la vie privée depuis 2015. Par conséquent, bien qu'elle déclare que la solution ait été conçue en tenant compte de la vie privée, les politiques d'Estimote ne valident pas cette conclusion.

4. LA VALEUR DE JUSTICE SOCIALE ne peut de même être oubliée au moment où la vulnérabilité de chacun face à la maladie n'est pas la même pour tous et oblige à privilégier une technologie accessible pour chacun et, d'abord, aux plus démunis face à la maladie. L'utilisation de systèmes de traçage automatique exclut les personnes qui ne disposent pas de téléphones portables ou ne peuvent utiliser le bluetooth ; des systèmes d'intelligence artificielle prédictifs peuvent amener à ostraciser certaines catégories de personnes dont on peut suspecter l'affectation par le virus ou certains quartiers où résident des personnes contaminées (souvent membres de groupes déjà marginalisés). Il ne s'agit pas simplement de protéger les données d'individus, mais d'éviter des discriminations par rapport à des groupes de personnes. Enfin, la valeur de dignité exclut une surveillance de tous les instants et l'ostracisme public vis-à-vis des personnes atteintes de la maladie (les QR codes de couleur utilisés en Chine). Ces valeurs doivent être prise en considération dès le design des solutions technologiques et tout au long de leur vie (*Ethics by design*). Cette valeur trouve sa déclinaison dans le critère n° 4 de la grille multifactorielle.

ÉQUITÉ ET NON-DISCRIMINATION

L'outil de traçage de contacts du gouvernement indien, **Aarogya Setu**, compte déjà plus de 114 millions d'utilisateurs inscrits. Par rapport à la population totale de 1,3 milliard d'habitants, ce chiffre peut être mis en perspective en soulignant qu'il ne représente que 8,7 % des habitants. Le gouvernement a annoncé récemment que l'adoption de l'application devait se faire suivant la règle de « l'effort raisonnable » dans les sociétés privées, diluant sa position initiale sur son adoption obligatoire, mais son utilisation est encore imposée par de nombreux employeurs et dans des contextes comme les transports ferroviaire et aérien. Compte tenu de la nature obligatoire de l'outil dans certains contextes et de la possibilité de sanctions, on ne peut s'empêcher de noter que le nombre de personnes concernées par ces mesures seules dépasse le nombre d'habitants de la France et de Singapour, mises ensemble. Il constitue un risque de discrimination à grande échelle, menant à des situations où les employés/personnes n'auraient pas d'autre choix que d'installer la solution ou risquer de perdre une possibilité d'emploi. Alors qu'un comité établi par le gouvernement a mis en place un protocole visant à régir l'utilisation des données par l'application, l'absence d'une loi exhaustive sur la protection des données et d'un cadre législatif pour la solution soulève des craintes quant aux conséquences juridiques et au risque de nuire aux utilisateurs. De plus, il existe un risque général d'utilisation aux fins de surveillance, de faux positifs et de faux négatifs et d'accès non autorisé aux données (y compris des données sur la santé) par des tiers.

Estimote est un dispositif portable très simple. Aucune application n'est requise, et il ne s'approprie donc pas le téléphone de l'utilisateur, ni ne contient (probablement) d'informations personnelles de l'utilisateur. Il peut également être utilisé par des personnes handicapées ou celles qui ne maîtrisent pas les nouvelles technologies. Il suffit d'appuyer sur un bouton pour indiquer qu'on est infecté. L'appareil possède également des alertes, visuelles et auditives, pour informer son utilisateur qu'il ne respecte pas les directives de distanciation physique (qu'il est trop proche d'une autre personne) ou qu'il a été exposé à une personne infectée et doit donc prendre les mesures appropriées.

Il est important de relever que certains critères additionnels pourraient avoir un impact significatif sur l'équité ou la non-discrimination, à savoir : i) le contenu des notifications, ii) des sanctions (le cas échéant) en cas de non-respect de ces notifications (y compris, mais sans s'y limiter, des sanctions légales, mais aussi liées au retour au travail, notamment après une période d'absence autorisée), iii) des limites que posent le respect et le non-respect des règles (par exemple, les contraintes financières et les circonstances socioéconomiques).

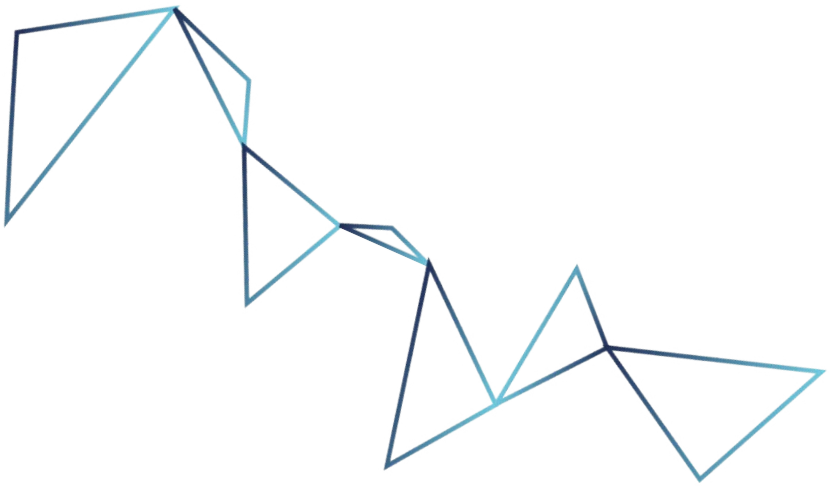
TerraHub a développé une solution blockchain permettant aux employés de partager, sur une base volontaire, des informations relatives à leur état de santé ou des certificats. Un algorithme propriétaire est ensuite utilisé pour analyser ces éléments, afin de transmettre à l'employeur un résultat se présentant sous la forme binaire d'un résumé « OK » ou « NOT OK », afin d'accompagner les mesures de reprise d'une activité économique post-confinement. Ce fonctionnement pose légitimement des questions en termes de transparence et d'explicabilité. D'une part, il n'est pas garanti à l'employé qu'il puisse avoir accès aux mécanismes de fonctionnement de cet algorithme, si bien qu'il paraît difficile pour lui de comprendre les critères sous-jacents ayant permis d'aboutir à un résultat « OK » ou « NOT OK », et donc éventuellement de les contester. Cela pourrait, d'autre part, aboutir à de conséquences importantes si cet outil algorithmique d'aide à la décision détermine par exemple les conditions d'accès au lieu de travail (obligation de rester chez soi en cas de résultat négatif, quelles mesures complémentaires seront entreprises en cas de test positif comme négatif, etc.), sans évoquer les risques de faux positifs et faux négatifs. Par ailleurs, l'usage secondaire de ces données, aussi bien des comptes rendus « OK/NOT OK », que des données personnelles stockées hors de la chaîne mérite un encadrement clairement défini, pour éviter tout détournement dans leur usage par des tiers.

5. L'ÉVALUATION DE L'INTÉRÊT GÉNÉRAL DOIT ÊTRE INCLUSIVE ET RÉUNIR TOUTES LES PARTIES PRENANTES. Il importe qu'une place soit laissée à la discussion publique au sein d'un forum réunissant toutes les parties prenantes : corps médical, représentants de la société civile (en particulier, des groupes vulnérables ou marginalisés), des entreprises, du milieu éducatif, etc. Il ne peut être question d'abandonner aux seuls experts la décision du choix d'un système plutôt que l'autre mais d'ouvrir à la discussion les choix et d'en imposer l'évaluation tant sur les plans techniques (*ethics by design*) que sur les autres plans (psychologique, socioéconomique,...). En définitive, c'est l'autorité politique constitutionnellement désignée comme compétente qui, après des organes « indépendants » requis, tranchera et fixera les contours et le mode de fonctionnement de l'outil technologique. En toute clarté vis-à-vis de la population et afin d'obtenir (et maintenir) sa confiance (notamment comment éviter que les technologies de sécurité ne deviennent des technologies sécuritaires), l'autorité publique expliquera, en minimisant autant que possible l'usage d'un langage paternaliste, les raisons des choix posés et le contenu des décisions, y compris les modèles utilisés par les algorithmes d'IA éventuellement retenus. À cet égard, nous ne pourrions admettre que les choix technologiques soient dictés par des acteurs qui n'opèrent pas de manière transparente et avec le souci d'une évaluation éthique. Cette valeur trouve sa déclinaison dans les critères n° 2 et n° 6 de la grille multifactorielle.

RESPONSABILISATION

Les données pseudonymisées nécessaires à la formation de modèles statistiques et épidémiologiques prédictifs de l'application COVI seront stockées dans un serveur sécurisé dont l'accès sera limité à certains chercheurs en IA qui entraîneront ces modèles. MILA travaille actuellement à la création d'une fiducie à but non lucratif, COVI Canada, pour le stockage des données. Selon le livre blanc sur l'application COVI, « la fiducie de données aurait des règles ouvertes sur sa gouvernance, un accès au code et aux modèles épidémiologiques agrégés, et serait continuellement surveillée par son conseil d'administration et des comités d'experts internes et soumise à des évaluations externes de groupes universitaires indépendants et de représentants gouvernementaux, pour veiller à ce qu'elle reste fidèle à sa mission. Elle serait démantelée à la fin de la pandémie et les données personnelles seraient détruites. La fiducie de données serait chargée de déterminer qui pourrait avoir accès aux données, et ce, uniquement dans le cadre de sa mission, à savoir mieux servir la santé et la vie privée des citoyens en gérant ces données et en les utilisant pour faire des recherches. La mission unique et le caractère non lucratif de la fiducie de données, ainsi que les mécanismes de contrôle de ses décisions, constitueraient une bonne défense pour veiller à ce que les données ne soient jamais utilisées par des entreprises ou des gouvernements à des fins de surveillance. »

Outil d'aide technologique à la stratégie de gestion de risques post-COVID, l'application COVI n'est ainsi pas une application développée par une entreprise privée, mais par un organisme indépendant à but non lucratif, constitué principalement de chercheurs. Or, OBNL ne signifie pas nécessairement absence d'intérêts privés. Aussi, pour qu'une telle orientation soit avantageuse, elle devra favoriser une plus grande transparence quant aux caractéristiques techniques et aux algorithmes mobilisés par l'application, principe qui constitue un enjeu central relativement aux outils numériques. Cette transparence sera par ailleurs favorisée par le fait qu'il s'agit d'une application en *open source* et que le concepteur affiche un souci clair en faveur d'un développement responsable des produits issus de l'intelligence artificielle. Les concepteurs de l'application se sont par ailleurs accordés pour soumettre l'application COVI à de multiples évaluations par des regards externes, notamment un comité d'éthique spécialement constitué à cette fin, mais aussi la Commission d'éthique, science et technologie (CEST) du Québec et les chercheurs de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA). Non seulement essentielle en termes de transparence, une telle ouverture à des évaluations externes, tout comme le fait qu'elle soit développée par une équipe interdisciplinaire qui inclut des experts dans le champ des technologies et de la santé, entend favoriser la meilleure prise en compte possible des différents enjeux contextuels et sociétaux que pourrait soulever le recours à cette application.



L'**application Coalition** de traçage de contacts, développée sous la gouverne de la société américaine Nodle, offre un service permettant à une personne de s'autodéclarer positive ou négative à la COVID-19. Les utilisateurs se déclarent eux-mêmes comme « positifs » et peuvent choisir de notifier le système de leur état. Pour ce faire, contrairement à d'autres solutions, il faut qu'une autorité de la santé intervienne ou qu'un test soit réalisé, en fonction de l'information actuelle, ce qui pourrait entraîner des notifications erronées ou même malveillantes. C'est d'autant plus important que l'autodéclaration déclenche la notification aux contacts.

DONNÉES OUVERTES, CONCURRENCE LOYALE ET PROPRIÉTÉ INTELLECTUELLE

TraceTogether est une application qui repose sur la technologie Bluetooth et qui a été développée par le ministère de la Santé de Singapour qui exploite le protocole BlueTrace dans le but d'accroître et d'améliorer l'efficience et l'efficacité du traçage de contacts. Le protocole BlueTrace est en *open source* et le ministère de la Santé de Singapour a indiqué que d'autres pays sont libres de le mettre en œuvre localement s'ils le jugent approprié. De fait, ce protocole comprend l'application COVIDSafe lancée par le ministère de la Santé du gouvernement australien. Dans le contexte de la pandémie, cet exemple illustre la valeur des modèles d'octroi de licence en *open source* et des technologies interexploitables.

DP-3T est un protocole décentralisé destiné à une application de traçage des contacts hébergée sur les téléphones intelligents utilisant le système d'exploitation de Google (Android) ou d'Apple (iOS), et conçu pour faciliter le traçage de contacts dans la population en général. Il s'appuie sur une architecture pouvant être déployée à l'échelle internationale. L'application DP-3T a été diffusée comme source ouverte. Les catégories de données sont des identités éphémères compactes pouvant être transmises au moyen des protocoles de la technologie BT LE. La publication complète a supplanté l'architecture système pour permettre cette portabilité. Compte tenu de la nécessité d'évaluer la mise en œuvre actuelle de DP-3T à l'échelle nationale, nous sommes dans l'incapacité d'examiner les normes d'interopérabilité actuelles. Toutefois, l'approche adoptée par les auteurs du protocole en tant que tel témoigne bien du partage des données et de l'application des normes.

6. LA PROPORTIONNALITÉ ET LA SÉCURITÉ DES SYSTÈMES MIS EN PLACE. Cette valeur doit guider le choix du système technologique, si du moins un tel système devait être retenu. A cet égard, on soulignera le principe de minimisation des données collectées tant dans le contenu (par exemple, en cas de base de données centralisée, doit-on enregistrer le numéro de registre national des personnes infectées et en contact ? Doit-on mentionner le nom du médecin à la base de la constatation de l'infection ?). On soulignera l'exigence de qualité des données collectées et traitées mais surtout les limites quant à la durée des traitements. La tentation de conserver les systèmes technologiques mis en place afin de combattre l'urgence du moment est grande. La pérennité des solutions inventées en cas de crise (l'exemple des attentats terroristes de septembre 2001 peut être cité) est souvent justifiée par l'intérêt de l'innovation et l'effectivité notable que la technologie peut apporter à la loi. La nécessité du respect strict de la finalité, qui a présidé à la mise sur pied des systèmes, doit être garantie. Elle implique que la gestion d'un dispositif de crise sanitaire exploitant des données personnelles de santé soit confiée à des organes réunissant des professionnels de santé et les parties prenantes (p. ex., groupe de patients). Le respect de ces principes ne peut être assuré qu'en conférant aux citoyens le droit de vérifier leur respect. Enfin, la sécurité et la fiabilité des dispositifs constituent un point crucial. En effet, si la solution est facilement piratable ou manipulable ou si elle ne fonctionne pas comme prévu ou est utilisée pour des usages non consentis, alors l'acceptation et la confiance dans cette solution sera largement entamée. Cette valeur trouve sa déclinaison dans le critère n° 5 de la grille multifactorielle.

FIABILITÉ ET SÉCURITÉ

Pour ce qui est de l'application **Corona-Datenspende**, des tiers connaissant le pseudonyme d'un donneur de données pourraient extraire du serveur de RKI le contenu de son jeton d'authentification et acheminer davantage de données à l'application RKI à l'égard de ce pseudonyme, par exemple, le nombre de pas ou toute autre donnée liée à ses activités. Des tiers pouvant également brancher leur propre moniteur d'activité à l'application pourraient également réussir à lier les données sur leur état de santé au pseudonyme d'un autre utilisateur. Ces risques ne doivent pas être considérés comme purement théoriques du fait qu'ils ne nécessitent pas des compétences techniques très poussées.

Nous recommandons que des mesures de protection additionnelles soient adoptées en ce qui a trait à la suppression des données. Selon le protocole **DP-3T** proposé actuellement, les données doivent être supprimées des serveurs après 14 jours, et la solution va se décomposer elle-même lorsqu'elle ne sera plus requise et que les utilisateurs cesseront de téléverser leurs données dans le serveur Autorisation, ou cesseront de l'utiliser. Nous proposons d'ajouter une disposition d'extinction en vertu de laquelle les données seront automatiquement supprimées lorsqu'un organisme externe (comme l'OMS) déclarera la fin de la pandémie.

ADOPTER UNE GOUVERNANCE INCLUSIVE ET PARTICIPATIVE

Au-delà du débat sur l'efficacité intrinsèque de chaque technologie comme outil de prévention de la pandémie, il convient de rappeler qu'en raison de sa nature, le risque ne peut être combattu que par un **effort collectif**. Aucun outil de protection face au COVID-19 ne produira donc les résultats escomptés s'il n'est pas intégré à une démarche de gouvernance publique inclusive et participative, qui responsabilise et rassure toutes les populations concernées. Il ne revient pas à l'État seul ou aux individus, aux syndicats professionnels ou aux seules entreprises d'imposer leurs solutions sans concertation ni coordination plus large, au risque de ne voir celles-ci rester sans effet.

Ce besoin d'une gouvernance participative et inclusive des dispositifs technologiques doit être mis rapidement à l'ordre du jour, à tous les niveaux de la société civile : entreprises, institutions publiques, corps intermédiaires, gouvernements... En effet, les risques et les conséquences d'oppositions stériles entre « individus » et « État », « entreprises » et « institutions publiques », « fédérations » et « administration » sont trop importants pour ne pas étudier **la place que les corps intermédiaires pourraient prendre, chacun à son niveau décisionnel**. Si cette demande n'a pas attendu la crise actuelle pour s'exprimer, elle acquiert aujourd'hui une visibilité et une réception publique sans précédent dans l'histoire de nos démocraties à l'ère du numérique.

Mais que faut-il entendre ici par gouvernance ? S'intéresser aux processus décisionnels ne nous focalise pas tant sur les choix à opérer que sur **la façon dont nous prenons ces décisions et imaginons ces mesures**. Car si les contextes de guerre ou de terrorisme ont, dans le passé, permis de justifier le recours à des pouvoirs d'exception, la présente crise sanitaire offre la possibilité pour le référentiel du soin (cf. Partie I) et une éthique du *care* de prendre le relai.

On peut donc considérer la crise actuelle comme **une opportunité pédagogique** pour renforcer la capacité des individus, des groupes et des collectivités à participer aux décisions qui les concernent. Un tel processus permettra aux citoyens de mieux s'adapter aux circonstances changeantes, et de contribuer à la résilience de notre société face aux crises futures.

Cette conception très active et participative de la gouvernance gagnera à être déployée à plusieurs niveaux. D'abord, au **niveau politique**, pour gérer la crise. À cet égard, on note des approches très variées d'un pays à l'autre, allant de l'interventionnisme à un certain laisser-faire. Si une intervention rapide et coordonnée a souvent permis un meilleur contrôle de la pandémie, les initiatives ayant par la suite conduit à une gestion plus efficace de la crise semblent celles où les communautés et les groupes professionnels interpellés (corps intermédiaires) ont été écoutés. Au-delà de la dimension représentative que permettent les élections démocratiques et de la possibilité de ne pas adopter une mesure proposée, c'est le rôle actif des citoyens qui permet une dynamisation du social et du politique, fondée sur des choix éclairés par les différentes attentes et réalités du terrain.

Tout en jouant un rôle central dans la prise de décisions rapides et la coordination des actions à l'échelle nationale, **l'État doit donc aussi encourager les initiatives locales mais également sectorielles** - que ce soit par des comités de gestion de crise dans différents milieux professionnels ou des regroupements pour favoriser la relance économique. L'exécutif peut ainsi assurer un ajustement constant de ses orientations et politiques à la lumière de la rétroaction provenant de ces initiatives. Au Québec, par exemple, de nombreux comités d'experts ou de concertation ont été mis en place afin de gérer la crise sanitaire, afin de permettre un meilleur alignement entre les consignes nationales et les actions menées dans divers milieux. Des difficultés ont été observées lorsque ces groupes d'acteurs ne se sont pas sentis suffisamment impliqués ou n'ont pas été mobilisés, ou lorsque les autorités ont annoncé des orientations et mesures qui ne trouvaient pas appui dans leurs travaux et recommandations.

La perspective participative de la gouvernance peut également être déployée dans la façon dont nous opérons nos **choix technologiques**. Dans le présent rapport, nous nous sommes penchés sur le cas plus particulier des applications de traçage proposées dans différents pays et par différents concepteurs. Dans tous les cas, une attention

particulière est portée à la possibilité individuelle de consentir ou non à utiliser les applications en question et à transmettre des données personnelles. L'adoption d'un processus de **gouvernance inclusive** permettra, selon nous, d'emporter **l'adhésion volontaire** des publics concernés à l'usage d'un outil technologique. Cette conception nous paraît donc incompatible avec le choix opéré par certains gouvernements de rendre obligatoire l'utilisation d'applications.

À ce titre, il ressort de notre étude que la plupart des initiatives se fonde sur le recueil du consentement pour justifier une protection adéquate. Ce consentement peut-il pour autant être réellement considéré comme libre et éclairé ? Face à la pression sociale pour utiliser de tels dispositifs, que ce soit sur un lieu de travail ou dans un immeuble d'habitation, l'autonomie de la personne concernée et le caractère « réellement » volontaire de l'adoption des dispositifs techniques semblent devoir être sérieusement nuancés. Certains commentateurs avertis indiquent qu'il ne pourrait s'agir tout au plus que d'un consentement induit.

Par conséquent, au-delà d'un examen de chaque application numérique, c'est aussi notre rapport plus large à la technologie que l'on doit examiner. La présente crise nous amène ainsi à (re)penser toute notre **gouvernance technologique**, c'est-à-dire nos orientations quant à la place et la façon de gérer les outils technologiques dans nos sociétés et dans nos organisations. Il s'agira donc de mettre en place des mécanismes qui permettront d'engager la discussion sur la pertinence sociale des technologies disponibles, et lorsqu'elles sont jugées désirables, de tracer les lignes d'acceptabilité sociale face à celles-ci et de faire émerger les valeurs, principes et balises que nous souhaitons pour en encadrer les utilisations.

Plus cette **inclusion aura lieu en amont, c'est-à-dire dès le stade d'émergence d'une technologie**, en questionnant le pourquoi de celle-ci avant d'envisager son comment, plus on sera en mesure d'intégrer dans les choix de conception une large étendue de préoccupations, tant pour la santé publique tant que pour les utilisateurs, qui peuvent être des consommateurs finaux tout autant que des collaborateurs ou des communautés. Cette inclusion aux stades précoces de développement d'une technologie permet d'anticiper des problèmes ou défis qui surviendraient nécessairement plus tard et ainsi de minimiser les complications liées à des ajustements à des stades plus avancés. Ceci dit, tous les enjeux ne pourront, bien évidemment, être découverts à l'avance et il importera aussi d'assurer, tout au long du cycle de vie de la technologie retenue, des retours d'expérience, afin de permettre des ajustements constants, au regard des enjeux pratiques soulevés par l'utilisation d'une technologie.

C'est là le sens fort de ce que nous qualifions de design éthique (ou *ethics by design*) ; une notion qui va bien au-delà de la simple énonciation de principes éthiques généraux à respecter et couvre un champ beaucoup plus large que la *privacy by design*. On cherche ici plutôt à permettre la **contextualisation des choix technologiques et à prendre en compte la multiplicité de conséquences et d'enjeux éthiques** qu'ils portent. À cet égard, la situation actuelle met en lumière le fait qu'un contexte de crise sanitaire, qui appelle **soin et solidarité**, peut amener à **revoir la priorité accordée à certaines valeurs**. On a, par exemple, souligné à maintes reprises le fait que des compromis relatifs aux applications de traçage jugés acceptables dans certains pays ne le seraient pas en Europe ou en Amérique du Nord, notamment en raison de possibles atteintes aux libertés.

Le risque d'opposer dogmatiquement l'affirmation des droits et libertés de l'individu aux besoins de la santé publique et de la protection de l'intérêt collectif reste réel et piégeant, en particulier au sein de notre culture occidentale moderne, centrée sur la promotion de l'individu. Inversement, relève toujours du pouvoir d'un collectif (famille, communauté, institution,...) la capacité de restreindre, à condition d'en démontrer la nécessité et la proportionnalité, les droits et libertés de ses membres (en invoquant, par exemple, un argument de bien commun comme la santé publique). De telles mesures politiques s'observent couramment dans certains pays, où la privation des droits et libertés individuelles ne relève pas d'un régime d'exception. Face à ce qui est présenté comme un dilemme, nous pensons que nous devons tabler sur l'intelligence collective et adopter ce que nous avons appelé le référentiel de soin pour nous situer sur un chemin de crête et d'équilibre entre les deux dogmatiques. Des sondages récents montrent en effet que, dans le contexte actuel de pandémie, certains citoyens seraient pourtant disposés à faire des compromis pour assurer la santé et la sécurité de leurs proches et de leurs aînés. Cela ne signifie pas qu'ils soient

pour autant disposés à renoncer au respect de leur vie privée. Cela implique plutôt la nécessité de répondre de façon créative au défi **d'articuler sécurité et santé publique avec le respect de la liberté individuelle et de la vie privée** afin qu'elles se renforcent mutuellement. En contexte de pandémie, cela signifie penser des outils technologiques visant à augmenter la sécurité (sanitaire) collective, qui intègrent de robustes garde-fous en matière de respect de la vie privée et des données, tout en les articulant avec des préoccupations d'équité et de justice sociale. Si nous arrivons à relever ce défi, cette nouvelle sécurité collective signifiera plus de liberté individuelle.

Dans tous les cas, l'idée est d'éviter les choix définitifs, mais utiliser plutôt un processus raisonné, transparent et itératif qui permettra une évaluation continue de nos choix en matière de technologie. Des instances tierces (*trusted third parties*), par exemple des **organismes de vérification** ou de **certification indépendants**, pourraient avantageusement être mis à contribution pour assurer un tel suivi. Leur action devrait alors se conformer aux orientations identifiées via les mécanismes de participation des parties prenantes à la gouvernance du dispositif.

L'IMPACT DU COVID-19 SUR LES ENTREPRISES

Si naturellement, le recul manque encore pour analyser les conséquence du COVID-19 sur le monde de l'entreprise, des basculements sont apparus et doivent être pris en compte pour guider le choix et la mise en oeuvre de solutions technologiques de sortie de crise.

Avec cette épidémie, la fragilité dans le monde du travail ne concerne plus uniquement quelques individus isolés, c'est toute la « ressource humaine » qui s'est trouvée, du jour au lendemain, empêchée d'assurer son travail quotidien dans des conditions normales. Des promoteurs de l'automatisation et de la robotisation ont pu y voir une confirmation **des théories visant à remplacer ce facteur humain si fragile**. Si aucun domaine ne semble à l'abri d'une automatisation partielle ou totale, la réalité immédiate est tout autre dans la mesure où l'activité de base des sociétés frappées par le virus n'a pu tenir que par le travail - souvent « invisibilisé » - de métiers parmi les moins valorisés. Par ailleurs, au regard des perspectives d'une hausse inédite du chômage dans les prochains mois, voire années, le choix du tout automatisé risque de provoquer de vives tensions sociales. Enfin, il convient de rappeler que **l'automatisation apparente des tâches humaines ne fait parfois que déplacer ou dissimuler le travail humain**.

Mais la pandémie a aussi mis en évidence la fragilité et la **vulnérabilité des théories de *lean management*, du zéro stock et des flux tendus**. Les chaînes d'approvisionnement tendues à l'échelle planétaire ont montré, comme l'image de la chaîne le suggère, que la rupture d'un seul maillon produit un effet domino aux impacts mondiaux. Les très fortes variations de demandes à la hausse (masques, respirateurs) ou à la baisse (tourisme) ont brusquement fait dérailler les règles du libre-échange, au point que certains États - y compris les plus libéraux - ont dû prendre des mesures pour fixer les prix. À n'en point douter, les **questions de relocalisation et de ré-industrialisation** et leurs corollaires sociaux vont se poser avec acuité pour toutes les économies du monde avec, en toile de fond, le souhait de retrouver une souveraineté économique et technologique, impliquant de vastes conséquences géopolitiques.

Dans cette crise, il est probable que la théorie de **la « destruction créatrice » trouve de nombreux cas d'application**. Le secteur automobile, par exemple, déjà perturbé depuis plusieurs années en raison de l'évolution des modes de consommation et d'une perte de réputation au gré de diverses affaires, voit déjà, la crise à peine passée, une accélération de sa « réorientation ». Comme d'autres secteurs qui étaient les fleurons des économies puissantes (transport aérien, aéronautique, distribution...), le secteur de l'éducation lui-même, avec son pivotage brutal et plus ou moins bien réussi vers des pratiques d'enseignement et de recherche à distance, va aussi connaître de profonds changements. De même, les services publics soumis, parfois à l'excès, à la privatisation, retrouvent aussi une définition plus claire de leurs véritables enjeux collectifs.

Mais le phénomène le plus immédiat et massif pour l'économie reste la généralisation brutale du **télétravail**. Il ne s'agit pas d'un sujet nouveau, mais l'ampleur mondiale du passage au travail à distance touche le coeur de la valeur et de la représentation sociale du travail pour définitivement sceller un changement profond dans l'organisation du travail salarié, hérité du fordisme. De nombreux témoignages évoquent **le gain de productivité** issu de la suppression des temps de transports et d'une organisation plus rigoureuse, liée aux modes de communication numériques. Découvrir collègues et clients dans leur environnement familial peut avoir contribué à des rapprochements. Pourtant, nombreux sont ceux qui pointent **le manque de temps de socialisation** et de rencontres en personne, qui diminue le sentiment d'appartenance à une équipe ainsi que la sérendipité nécessaire aux processus d'innovation. Cette nouvelle organisation ne permet plus les modes de contrôle de salariés qui seraient « au travail », issus du Taylorisme et nécessite de **repenser en profondeur l'organisation des entreprises**, pour l'adapter à cette période de crise. Bien sûr, les effets de ces changements de pratiques sont ambivalents mais, en faisant éclater une partie des cadres réglementaires et des consensus sociaux, ils modifient les rapports de force en accentuant le pouvoir de l'employeur qui peut accroître sa rentabilité, penchant progressivement vers **une plateformisation des rapports du monde du travail**.

Les mois et années à venir inaugurent une situation totalement inédite. Quelle qu'en soit l'issue, impossible à estimer à ce stade, la notion de **résilience individuelle et collective** sera essentielle. À l'aune de l'histoire humaine et de son développement, l'atout de l'humain a toujours été sa capacité à agir collectivement et donc politiquement face à des ressources limitées. Plus que jamais, **la capacité des économies à survivre s'appuiera sur la capacité humaine à agir ensemble en révisant sans doute la tension entre productivité et résilience**.

EXERCER LA GOUVERNANCE DES OUTILS TECHNOLOGIQUES EN ENTREPRISE

Le déconfinement et le retour des employés sur leur lieu de travail soulèvent la nécessité pour les entreprises de se doter de dispositifs, technologiques ou non, qui permettront de **protéger chacun de toute infection et qui garantiront la confiance dans l'autre**, prérequis à la reprise des activités. Les analyses précédentes ont identifié un éventail de technologies susceptibles d'appuyer les mesures de distanciation sociale (voir notamment l'encadré sur les technologies Bluetooth/iBeacon et la présentation de diverses technologies d'accès sur les lieux du travail). Notre objectif n'est pas de détailler les modalités pratiques de déploiement de chacune d'entre elles, mais d'identifier les caractéristiques d'une gouvernance appropriée et efficace. Par ailleurs, les leçons apprises pendant le confinement peuvent amener la volonté de modifier les processus et l'organisation du travail en entreprise.

Notons d'emblée les **spécificités de la gouvernance en entreprise**. Les relations entre employés sont à la fois plus proches et souvent vécues de manière plus intense que dans la société. Le retour au travail est le moment d'une confrontation des expériences vécues différemment par chacun face au coronavirus. Cette confrontation n'est sans doute pas aisée, tant la période de confinement peut avoir changé les personnes et leurs relations vécues à distance. Il importe dès lors, au niveau local, de **créer ou recréer des espaces de dialogue et d'écoute bienveillante** afin que chacun puisse s'exprimer sur la réalité qu'il a vécue et, le cas échéant, sur la façon dont la distance imposée renouvelle la conception de son travail à l'intérieur de l'organisation.

Il est clair qu'un retour du virus au sein de cette communauté mettrait en cause la responsabilité de la direction, risquant d'entraîner le droit de retrait, dans la mesure où la sécurité au travail sera déclarée par les employés comme insuffisante. Les mesures liées à la crise sanitaire ne font pas partie de l'activité normale de l'entreprise et touchent la santé, les relations, voire l'intimité des personnes. **Le lien de subordination risque donc de ne pas suffire à les faire adopter** efficacement. Or, on a montré les risques de contournement des mesures qui seraient jugées inadaptées, imposées de façon unilatérale ou trop contraignantes. Pour la direction d'une entreprise, il s'agit donc à la fois de **rassurer les collaborateurs et les clients ou fournisseurs** amenés à fréquenter les locaux, tout en pouvant compter sur eux pour l'application stricte des mesures. Bâtir cette **confiance réciproque** nécessite de mettre en place un mode de gouvernance adapté. En l'absence de règles provenant de l'extérieur telles que législations, directives émanant des régulateurs ou d'organismes professionnels, il s'agira de **bâtir un cadre normatif commun** et donc de discuter la hiérarchisation des principes à appliquer et les contraintes à imposer. En effet, s'ils doivent choisir entre sécurité et respect des libertés individuelles, les collaborateurs et clients feront très probablement le choix de la sécurité, premier degré de la pyramide des besoins de Maslow. Mais cette décision ne se prendra pas sans regret ni acrimonie et risque d'entacher l'image de la direction.

Or, **les structures du dialogue social ne sont pas adaptées à une telle situation de crise** : même des instances comme le CHSCT en France ou la médecine du travail ont rarement (à l'exception de quelques secteurs spécifiques) à statuer sur des mesures pouvant impliquer la survie ou l'organisation structurelle de l'entreprise. Afin que ces discussions ne minent pas le climat social, il apparaît opportun de **constituer une instance multipartite de gestion de la crise sanitaire dans l'entreprise**. Celle-ci s'avérera déterminante dans la collecte des suggestions de solutions, dans la discussion des priorités, dans l'analyse des stratégies possibles et des dispositifs technologiques envisagés, et surtout dans l'adoption des mesures décidées. En effet, l'expérience de la gestion réussie de la crise sanitaire dans des pays comme Taïwan ou le Vietnam a montré l'importance du recours aux communautés et d'une gestion de proximité. Une telle instance de gouvernement du projet permettra une gestion éthique *by design*, c'est-à-dire dès la conception de la stratégie, et contribuera à créer, au sein de l'entreprise, une véritable **culture de l'éthique et de l'attention à la santé de l'autre**. Elle offrira, en outre, la possibilité de mettre en oeuvre des **dispositifs technologiques pensés du point de vue des utilisateurs**, qu'il s'agisse des collaborateurs ou des personnes amenées à fréquenter les locaux. Ainsi, par exemple, si un dispositif d'auto-diagnostic par questionnaire ou de contrôle de la température indique qu'un employé ne peut accéder à son lieu de travail, sa prise en charge doit être assurée, en le dirigeant vers des structures de santé à même de confirmer un diagnostic et de le soigner, ainsi qu'en

lui offrant les conditions d'un travail à distance, si c'est possible, ou des moyens de subsistance, tout en évitant toute stigmatisation.

Par ailleurs, l'importance des efforts qui seront demandés aux personnes (contrôle des accès, distanciation physique, mesures de désinfection…) et la nature des informations qui pourraient être collectées impliquent de traiter le processus de gestion de la crise sanitaire comme un **projet indépendant de toute autre mesure de sécurité ou de contrôle**. Bien que la tentation puisse être forte d'utiliser les outils mis en oeuvre pour affiner la gestion des ressources humaines (localisation des collaborateurs, calcul des temps de travail et de pause…), le processus de gestion de la crise sanitaire devra disposer de bases de données spécifiques, totalement étanches et protégées. Les données de santé du personnel ne peuvent être traitées par l'employeur. L**a finalité exclusive des données collectées devra être garantie** à ceux qui donnent leur consentement.

Enfin, un tel processus de gouvernance participative, fondé sur le dialogue, permettra de développer la **stratégie de gestion de la crise sanitaire et de retour à l'activité en mode agile** : des mesures pourront être testées et évaluées, en toute transparence, afin d'atteindre par itérations successives la situation optimale. En outre, si ce mode de gouvernance permet de déployer progressivement la stratégie, il offre aussi la possibilité de réduire les mesures puis de les arrêter quand ce sera possible, cette limitation dans le temps étant un facteur important de confiance et d'acceptabilité sociale.

CONCLUSION

Au vu du grand nombre d'inconnues quant au virus et aux facteurs de contagion, nos sociétés doivent se préparer à vivre avec la menace de résurgences de la pandémie. La sortie de crise attendue par la population nécessite donc de **passer d'un mode de gestion de catastrophe sanitaire à un processus de gestion de risque à moyen terme**. Les solutions technologiques d'aide au déconfinement et au redémarrage économique ne peuvent donc être étudiées que comme des éléments d'un processus plus large de gestion du risque, y compris notamment les mesures sanitaires, le soutien apporté aux personnes potentiellement infectées, ainsi que l'encadrement des différents types d'activités économiques et sociales.

Afin d'éviter de se trouver pris dans un réseau de doubles contraintes qui empêcheraient toute prise de décision, **un arbitrage entre les valeurs sous-tendant les choix et une hiérarchisation des principes que nous voulons collectivement voir respectés doivent être opérés**, en évitant de centrer le débat sur le seul respect de la vie privée. Dans cette situation exceptionnelle, **assimiler les données collectées ou utilisées dans la gestion du risque pandémique à des données particulièrement sensibles**, éventuellement placées sous mandat de gestion des établissements médicaux, pourrait offrir des garanties satisfaisantes.

Le **principe de nécessité** nous semble devoir être privilégié : si l'utilité d'une solution technologique est jugée trop faible au regard de ses conditions d'implémentation (par exemple, une application qui nécessiterait, pour être efficace, une utilisation par 60 % de la population, mais dont l'adoption reposerait sur le volontariat), il conviendrait soit de changer temporairement les conditions de son déploiement, soit de changer de stratégie en déployant une technologie différente.

Si le suivi du parcours des personnes potentiellement infectées est le mode de gestion habituel des épidémies, et si une application peut permettre son déploiement à grande échelle, d'autres approches apparaissent, comme **l'utilisation de modèles prédictifs d'évolution de la pandémie, permettant d'identifier les lieux et les situations à risque**. Là encore, des risques éthiques existent, comme celui de voir stigmatisés certains quartiers ou populations (souvent déjà vulnérables ou marginalisés), mais ils devront être mis en perspective de l'efficacité de la solution dans la préservation de la santé publique. Ainsi, le débat ne peut se concentrer sur les modalités de mise en œuvre d'une solution sans s'interroger sur le caractère idoine de cette solution.

La mise en œuvre de mesures permettant une gestion sur le moyen terme représente un défi dans des sociétés ayant développé une forte aversion au risque. Elle nécessite un accompagnement attentif de la part des pouvoirs publics. Cet accompagnement porte, tout d'abord, sur **la gestion et le partage de la responsabilité** : elle ne peut pas peser sur les seules épaules de l'individu, au risque de voir stigmatisées les personnes infectées ; cependant, elle ne peut pas non plus être uniquement endossée par le collectif, au risque d'assister à une déresponsabilisation des personnes les moins vulnérables, au mépris de la justice sociale.

Toute solution efficace passe donc par l'exercice de solidarités entre des citoyens engagés. Cela présuppose :

- Le **rôle de coordinateur de l'État** dans la détermination des priorités de la santé publique (par exemple, ouvrir ou non des secteurs de l'économie, ainsi que dans la détermination des caractéristiques des dispositifs technologiques et du type de données recueillies), et la promotion de normes facilitant l'interopérabilité à l'échelle nationale et internationale des dispositifs numériques. Les dirigeants d'entreprise, notamment, ne peuvent être laissés seuls face à

la responsabilité de choisir des mesures de déconfinement ou de gestion de l'activité en situation de crise sanitaire (avant la distribution massive d'un vaccin), dans le cadre d'un dialogue social qui pourrait devenir tendu. L'État devra également définir les ajustements visant à minimiser les effets discriminants ou les torts subis par certaines catégories de population face à l'emploi de tels dispositifs, par exemple, par la mise en place de politiques publiques visant à compenser les pertes de revenus pour les personnes ou communautés qui acceptent de déclarer qu'elles sont infectées.

- Le rôle des *standards bodies* ou groupes consultatifs pluridisciplinaires indépendants dans l'évaluation des dispositifs technologiques envisagés et le développement de normes consolidant l'ensemble des meilleures pratiques du développement et le déploiement responsable de ces nouvelles technologies et **facilitant l'interopérabilité à l'échelle nationale et internationale** de celles-ci.

- Le **rôle du secteur privé** dans le développement et le déploiement éthique et responsable de ces technologies et dans l'ensemble des mesures prises pour assurer la santé des employés et des clients, ainsi que la relance responsable de l'économie.

- Le **rôle de gestion des communautés** (communes, corps intermédiaires (association de quartiers, direction d'écoles, ...) dans l'application locale des mesures, afin de coller au plus près des réalités du terrain et de favoriser l'adhésion de la population.

- Le **rôle de chaque citoyen** dans l'adoption de mesures parfois très contraignantes mais à même de lutter efficacement contre la pandémie - qui passe par une responsabilisation individuelle, collective et équitable entre toutes les parties prenantes - et le désir de la grande majorité des citoyens de ne pas attraper le virus et de ne pas contaminer leurs proches.

La gouvernance des solutions technologiques retenues apparaît donc comme le facteur clé conditionnant leur succès ou leur échec. Elle doit refléter la gestion des responsabilités évoquée ci-dessus. Pour ce faire, une instance idoine doit être créée, qui doit être :

- **Multipartite :** En plus des députés et du gouvernement, légitimes garants de la représentation régionale et nationale, ainsi que des experts, l'organe spécifique de gouvernance et de contrôle du déploiement de solutions technologiques doit aussi accueillir des représentants de la société civile et des corps intermédiaires, à mêmes de susciter la confiance et l'engagement des citoyens.

- **Agile :** À mesure que la situation et la connaissance du virus et de ses modes de propagation évoluent, la solution retenue devra être adaptée par itérations successives.

- **Transparente et raisonnée :** Dans l'évaluation régulière et l'éventuelle modification des solutions envisagées, le processus de raisonnement et les arguments (ou données probantes) mobilisé doivent être expliqués et justifiés de façon transparente et compréhensible. Ceci est crucial pour la confiance de la part des parties prenantes dans les choix qui sont faits.

- **Temporaire :** Si le risque lié à la pandémie est appelé à durer, le caractère évolutif et itératif des solutions proposées devra permettre d'en réduire la portée, puis de les arrêter en temps voulu, sous le contrôle direct de l'instance de gouvernance.

ANNEXES

ANNEXE 1

LES RÉFÉRENTIELS MOBILISÉS SOUS COVID-19

Nos référentiels structurent nos compréhensions des phénomènes et notre façon de penser. Les imaginaires collectifs et les représentations sociales jouent un rôle prépondérant dans l'adhésion (l'acceptation ou le refus) des dispositifs technologiques en cette période de crise. Dès lors, il importe de rendre visibles les principaux imaginaires qui constituent les référents significatifs auxquels nous nous rapportons (plus ou moins consciemment) pour tenter de comprendre la crise que nous traversons et les solutions brandies. C'est à partir de cette explicitation que nous pouvons évaluer le niveau d'adéquation ou d'inadéquation des référentiels en présence dans la situation que nous traversons, et comprendre leurs effets sur nos relations aux technologies de traçage actuellement en débat. C'est aussi sur la base de cette explicitation que nous pouvons mettre à jour le cadre de compréhension et de communication le plus ajusté à la situation actuelle.

Dans un objectif partagé de lutte contre le COVID-19 et de reprise des activités sociales, culturelles et économiques, ce travail est un réquisit incontournable : nous ne pouvons pas assimiler purement et simplement la situation actuelle à des situations passées ou plus ou moins comparables, ni laisser les imaginaires que ces situations différentes ont pu produire. Tout décideur, tout collectif doit être capable de parler avec justesse des situations problématiques rencontrées, s'il espère leur trouver quelque solution adaptée. Dans ce but, il est essentiel de savoir quel imaginaire, quel registre de signification solliciter face à la situation actuelle.

Sans prétendre ici à l'exhaustivité, nous pouvons distinguer au moins cinq grands imaginaires sociaux, qui sont autant de référentiels sollicités dans la crise actuelle pour la revêtir de significations diverses :

1. LE RÉFÉRENTIEL DES GRANDES ÉPIDÉMIES PASSÉES
2. LE RÉFÉRENTIEL DU TEMPS DE LA GUERRE
3. LE RÉFÉRENTIEL DE NOS RELATIONS AVEC LA NATURE
4. LE RÉFÉRENTIEL DES SOCIÉTÉS DE LA SURVEILLANCE
5. LE RÉFÉRENTIEL DU SOIN

1 LE RÉFÉRENTIEL DES GRANDES ÉPIDÉMIES PASSÉES

Dès les débuts de l'expansion pandémique de COVID-19 sur le continent européen, l'ouvrage *La peste* d'Albert Camus s'est rapidement trouvé en rupture de stock, et les références aux crises épidémiques meurtrières (peste, choléra, sida, Ebola, grippe espagnole,...) qui nous ont marqué par le passé, se sont multipliées dans de nombreux articles et médias. Or, l'imaginaire lié à ces épidémies garde à juste titre mémoire de microbes aux effets dévastateurs, littéralement faucheurs de vie. Sans commune mesure avec la crise pandémique actuelle, ces épidémies partagent pour point commun d'être responsables de la disparition de pans entiers de populations. À titre d'exemple, au XIVe siècle, l'épidémie de peste noire en Europe emporte avec elle plus de 50 millions de vies, dont 25 sur le continent européen. À l'époque, 33 % de la population européenne disparaît en quelques années (1347-1351). Au XXe siècle, entre 1918 et 1919, l'Institut Pasteur estime que la grippe espagnole causa entre 20 et 50 millions de décès. Quant au virus Ebola apparu ces dernières décennies, s'il est un peu moins contagieux que SARS-COV-2, l'OMS estime son taux de mortalité à environ 50 % (oscillant en général entre 20 et 90 % selon les régions recensées de l'épidémie).

Ces quelques chiffres relativisent la létalité et la gravité de la pandémie COVID-19. Le nombre de personnes décédées au niveau mondial en raison d'une infection à SARS-COV-2 s'élève à ce jour à 350 000 (à date du 26 mai 2020). Son taux de mortalité est situé entre 0,5 et 3 %[1]. Cette estimation reste toutefois approximative, variable selon les sources, et largement débattue en l'absence de données suffisamment précises sur le nombre de personnes réellement infectées par le virus. Si SARS-COV-2 est jugé 10 à 20 fois plus létal que la grippe saisonnière, cette dernière tue depuis des décennies entre 290 000 et 650 000 personnes dans le monde[2], et son coût social et économique est considérable. Cette réalité avec laquelle nous vivons depuis de nombreuses années ne nous choque pas outre mesure (ne devrions-nous pas nous en inquiéter ?). Il en est de même du nombre de décès annuels dus aux affections respiratoires habituelles, qui oscille entre 2,5 millions et 5 millions à l'échelle mondiale. En 2016, les 10 principales sources de décès dûs à des maladies dans le monde se situaient au-dessus de la barre de 1,5 million de victimes. Les plus létales d'entre elles atteignaient entre 9,5 et 10 millions de décès[3]. Quant aux cancers et aux maladies cardiovasculaires, ils causent respectivement 9,6[4] et 17,7 millions de morts sur la planète chaque année[5].

Autant dire que l'impact mondial de COVID-19 reste objectivement limité au regard de ces quelques statistiques des causes de mortalités les plus fréquentes. Il est par ailleurs impossible à ce stade de savoir si les victimes directes de COVID-19 seront plus nombreuses que ses victimes indirectes (patients dont le suivi médical n'aura pas eu lieu, se sera interrompu ou aura été décalé pendant la période du confinement, décès dus aux effets de la solitude, conséquences psychologiques sur les populations les plus vulnérables, etc.). Mais à côté du souci pragmatique d'éviter l'étouffement du système hospitalier et de l'obligation de soin aux malades touchés par l'épidémie, l'imaginaire des grandes épidémies meurtrières auquel SARS-COV-2 est associé par des caractéristiques qu'il partage avec elles, participent des réactions et des craintes sociales dont il fait l'objet à l'échelle planétaire.

COVID-19 est bien une épidémie de dimension mondiale (pandémie) et d'origine virale. Elle partage un même champ de significations avec d'autres maladies virales : dans l'imaginaire collectif, les virus sont réputés pour être nuisibles, résistants aux antibiotiques, imprévisibles, sources de variabilité génétique et d'évolutivité imprédictible. Leur comportement, à la frontière du vivant et du non-vivant, en fait des êtres ambivalents, hybrides, inquiétants, générateurs de fantasmes et d'angoisses sociales. Leur traitement est plus complexe. Quel que soit son niveau (modéré) de gravité, la possibilité de vagues successives d'épidémies de COVID-19 alimente ces craintes en l'absence de vaccin et d'une connaissance éprouvée du virus. Les médias grand public constituent dans ce registre de puissantes caisses de résonnance pour ces craintes, en focalisant l'attention publique sur les effets les plus rares mais les plus dramatiques ou impressionnants de la pandémie.

Devant l'impuissance des technologies et des traitements médicamenteux à constituer à eux seuls des

[1] https://theconversation.com/coronavirus-deux-mois-plus-tard-que-sait-on-du-taux-de-letalite-du-COVID-19-133584
[2] https://www.who.int/fr/news-room/detail/14-12-2017-jusqu-%C3%A0-650-000-d%C3%A9c%C3%A8s-par-an-sont-dus-aux-affections-respiratoires-li%C3%A9es-%C3%A0-la-grippe-saisonni%C3%A8re
[3] https://www.who.int/fr/news-room/fact-sheets/detail/the-top-10-causes-of-death
[4] https://gco.iarc.fr/today/home
[5] https://www.who.int/fr/news-room/fact-sheets/detail/cardiovascular-diseases-(cvds)

barrières efficaces contre la pandémie, SARS-COV-2 requiert enfin des réactions de santé publique similaire aux grandes épidémies passées : prise en charge spécifique des cas mis à jour, mises en quarantaine, mesures de prévention des infections et de lutte, surveillance et recherche des contacts, traçage manuel des chaînes de propagation, mobilisation des laboratoires, conscientisation sociale aux gestes barrière, confinement populationnel, réorganisation des territoires en fonction de la stratégie de santé publique, etc. Or, ces pratiques sociales séculaires n'ont pas attendu l'ère des technologies numériques pour prouver leur utilité. Elles se sont forgées par l'action et l'intelligence collective des populations et, faute de mieux, se sont avérées aussi efficaces que possible dans l'épreuve des grandes épidémies passées.

L'imaginaire des grandes épidémies, du moins en Occident, ne renvoie donc pas naturellement au registre des nouvelles technologies numériques. Celles-ci sont absentes de cet imaginaire qui s'est constitué en Occident au contact des grandes épidémies passées. Remobilisé par la pandémie de COVID-19, cet imaginaire n'est donc pas *a priori* prédisposé à l'intégration de ces nouvelles technologies. La pauvreté de leur *curriculum vitae* dans la lutte contre les grandes épidémies en Occident leur confère toute la charge de la preuve, et laisse planer un certain scepticisme *a priori* quant à leur compétence en la matière. Tant qu'elles n'auront pas démontré leur efficacité réelle en matière de santé publique dans la crise actuelle, les attentes sociales à l'égard des nouvelles technologies numériques resteront prudentes.

2 LE RÉFÉRENTIEL DU TEMPS DE LA GUERRE

La crise actuelle fait aussi réémerger les souvenirs des périodes de privation et de lutte en temps de guerre. Des hommes politiques de premier plan ont volontairement rapproché les deux situations pour renforcer l'unité nationale face à COVID-19. Ainsi, le 16 mars 2020 lors d'une allocution solennelle, le président Emmanuel Macron annonce aux Français que des mesures de confinement sont nécessaires pour freiner la propagation de COVID-19, et déclare sur un ton grave: « Nous sommes en guerre ». Le 8 mai 2020, jour anniversaire de la capitulation de l'Allemagne nazie, c'est au tour de Boris Johnson, premier ministre britannique, de recourir au champ sémantique de la guerre. Dans une lettre publique adressée aux vétérans, il compare la pandémie de coronavirus au « nouveau combat » qu'il s'agit de mener avec « le même esprit d'effort national » que 75 ans plus tôt.

La convocation du vocabulaire martial et de l'imaginaire de la guerre s'appuie sur des similitudes indéniables entre les deux situations : l'état d'urgence, l'appel à l'unité nationale, la mobilisation des services de santé, la convocation de l'armée, la sollicitation de toutes les forces vives, le contrôle des mouvements de population (contrôle policier, suivi par les technologies), la course aux denrées de survie (pâtes, riz, lait, farine…), la fermeture des frontières, les réquisitions de matériel par la puissance publique, les mesures d'économie de guerre (réorientation et nationalisation de certaines activités du privé aux fins de la lutte contre COVID-19), etc. Le scénario de la crise actuelle ressemble bel et bien à un état d'exception que l'on peut retrouver déployé en temps de guerre, avec des mesures contraignantes qui touchent l'ensemble d'un pays.

La tendance à recourir au vocabulaire de la guerre dans la situation présente est encore renforcée par l'usage bien connu de la métaphore dans le langage médical, comme le rappelle Bernadette Bensaude-Vincent, philosophe et historienne des sciences :

> « La métaphore guerrière est depuis longtemps à l'honneur dans le monde médical. Elle remonte au XVIe siècle à l'époque où la médecine initiée par Paracelse – souvent nommée iatrochimie (médecine chimique) – a concurrencé l'ancienne tradition galénique1. Contrairement à la vision holiste de la maladie comme l'expression d'un déséquilibre des humeurs, la maladie est vue comme intervention d'un agent étranger sur l'organisme, qui infecte un organe particulier et que l'on peut éradiquer à l'aide d'une substance chimique spécifique. Cette conception de la maladie présuppose une nette distinction entre le dedans et le dehors, le soi et le non-soi qui s'applique de manière privilégiée au système immunitaire. D'où les descriptions très pédagogiques des défenses immunitaires comme une armée de soldats en lutte pour résister aux attaques de microbes. La médecine du XXe siècle, marquée par la découverte, puis l'utilisation massive des antibiotiques est l'âge d'or de cette médecine guerrière qui culmine avec le fameux slogan de « *war on cancer* » lancé par Richard Nixon en 1971. »[6]

[6] https://www.terrestres.org/2020/04/30/guerre-et-paix-avec-le-coronavirus/

Si l'usage courant du vocabulaire guerrier en médecine ainsi que les ressemblances entre le temps de la guerre et le temps de la pandémie de COVID-19 rendent possibles certaines comparaisons, le rapprochement voire la confusion entre les deux situations, font inévitablement de l'imaginaire de la guerre un cadre d'interprétation de la crise actuelle, où la technologie ne saurait être uniquement perçue comme un moyen de défense ou d'attaque contre un ennemi extérieur (le virus). Dans l'imaginaire de la guerre, la technologie est aussi au service du contrôle populationnel, du renseignement interne, du savoir et du pouvoir des uns sur les autres. C'est un instrument de canalisation des forces vives et de propagande au service des buts de la nation (déterminés par l'État). C'est un moyen de guerre en vue du maintien de l'unité nationale, un outil de prévention contre les risques insurrectionnels, une arme qu'un pays peut retourner contre lui-même (guerre civile) ou contre ses ennemis invisibles (guerres asymétriques). Le recours au vocabulaire guerrier est ainsi à double tranchant, car il importe avec lui, dans la situation actuelle, ses propres représentations de la technologie, non seulement comme arsenal et outil de guerre, mais aussi comme moyen de contrôle politico-idéologique des populations.

Mais sommes-nous réellement en guerre contre le COVID-19 ? Comparaison n'est pas raison, et les métaphores, comme les virus, colonisent à l'insu les esprits. Comme les études de linguistique, la philosophie du langage et les sciences cognitives l'ont mis largement en évidence dans la seconde moitié du XX[e] siècle, nos métaphores structurent nos réalités (voir à ce propos l'ouvrage fondationnel de John. L. Austin, *How to Do Things with Words*. Oxford: Clarendon Press, 1962. Voir aussi George Lakoff, Mark Johnson, *Metaphors we live by*, Chicago: University of Chicago Press, 1980.). Dis-moi quel est ton langage, je te dirai dans quel monde tu vis (Wittgenstein) ! Recourir à l'imaginaire de la guerre, même comme une métaphore, pour caractériser nos relations en société face à SARS-COV-2, conditionne un type de rapport au réel au détriment d'autres cadres de référence possibles. Une métaphore fonctionne comme un filtre au travers duquel la réalité nous apparaît sous un certain point de vue. La perspective n'est jamais que partielle, mais si l'on n'y prend garde, la métaphore devient totalisante : à travers le langage, les images et les symboles qu'elle met à disposition, l'imaginaire qu'elle sollicite façonne à ce point nos perceptions et nos actions que nous le prenons pour la réalité même.

> "Metaphors may create realities for us, especially social realities. A metaphor may thus be a guide for future action. Such actions will, of course, fit the metaphor. This will, in turn, reinforce the power of the metaphor to make experience coherent. In this sense metaphors can be self-

fulfilling prophecies. For example, faced with the energy crisis, President Carter declared "the moral equivalent of war." The WAR metaphor generated a network of entailments. There was an "enemy," a "threat to national security," which required "setting targets," "reorganizing priorities," "establishing a new chain of command," "plotting new strategy," "gathering intelligence," "marshaling forces," "imposing sanctions," "calling for sacrifices," and on and on. The WAR metaphor highlighted certain realities and hid others. The metaphor was not merely a way of viewing reality ; it constituted a license for policy change and political and economic action. The very acceptance of the metaphor provided grounds for certain inferences: there was an external, foreign, hostile enemy (pictured by cartoonists in Arab headdress) ; energy needed to be given top priorities ; the populace would have to make sacrifices ; if we didn't meet the threat, we would not survive. It is important to realize that this was not the only metaphor available. Carter's WAR metaphor took for granted our current concept of what ENERGY is, and focused on how to get enough of it. On the other hand, Amory Lovins (1977) observed that there are two fundamentally different ways, or PATHS, to supply our energy needs. He characterized these metaphorically as HARD and SOFT. [...] The SOFT ENERGY PATH uses energy supplies that are flexible, renewable, not needing military defense or geopolitical control, not destructive of the environment, and requiring only low capital investment, low technology, and unskilled labor. They include solar, wind, and hydroelectric power, biomass alcohol, fluidized beds for burning coal or other combustible materials, and a great many other possibilities currently available. Lovins' SOFT ENERGY PATH metaphor highlights the technical, economic, and sociopolitical *structure* of the energy system, which leads him to the conclusion that the "hard" energy paths—coal, oil, and nuclear power—lead to political conflict, economic hardship, and harm to the environment. [...] New metaphors, like conventional metaphors, can have the power to [re]define reality. [...] The acceptance of the metaphor [of war], which forces us to focus *only* on those aspects of our experience that it highlights, leads us to view the entailments of the metaphor as being *true*. Such "truths" may be true, of course, only relative to the reality defined by the metaphor." (George Lakoff, Mark Johnsen, *Metaphors we live by*, London, The university of Chicago press, 2003, p. 156-158.)

À l'instar du changement de paradigme auquel invitait Amory Lovins dans son débat sur l'énergie avec Jimmy Carter, l'enjeu de la crise actuelle relève aussi d'un conflit des imaginaires. Pour interpréter nos vécus et orienter nos actions face à SARS-COV-2, le référentiel de la guerre mobilise une métaphore classique et puissante. Mais n'existe-il pas d'alternative(s) à l'imaginaire de la guerre pour penser nos attitudes face à SARS-COV-2 ? Jusqu'à quel point la métaphore de la guerre est-elle légitime, et quels sont les points aveugles qu'elle nous masque par l'éclat de son apparente évidence ? Quel(s) imaginaire(s) alternatif(s) nous empêche-t-elle de solliciter ? En nous inscrivant dans un paradigme de conflictualité, de quelles relations aux autres et à la nature nous détourne-t-elle ? Enfin, ne nous prive-t-elle pas dans la crise actuelle d'une relation moins martiale, plus pacifique et apaisée aux technologies ? Un imaginaire technologique différent du registre de l'arme de guerre ou de l'outil de contrôle et de propagande ne serait-il pas envisageable, voir préférable face à un enjeu de santé publique ?

3 LE RÉFÉRENTIEL DE NOS RELATIONS AVEC LA NATURE

Nombre de publications sollicitent un autre imaginaire comme cadre de signification de la crise actuelle. Dans *Politique de l'amphibiose : la guerre contre les virus n'aura pas lieu*[7], Charlotte Brives, anthropologue des sciences et de la santé, chercheure au CNRS, souligne que l'histoire de l'immunologie et de l'épidémiologie sont chargées en références guerrières. Elle fait cependant remarquer que ces métaphores sont largement anthropomorphiques : elles projettent des traits humains sur des réalités qui n'en sont pas. La métaphore de la guerre attribue à des types d'êtres situés à des niveaux de réalité (microscopique) infiniment différents du nôtre un statut d'« ennemi extérieur », une « stratégie guerrière », des « intentions belliqueuses ». Or, le concept d'« ennemi » présuppose l'existence d'une intention malveillante. Si les virus sont engagés dans des relations profondément intimes avec les humains qui peuvent, dans certaines conditions, mettre leurs vies en péril, leur prêter une conscience (belliqueuse) et des intentions (guerrières) n'engage que ceux qui font ce pas.

[7] https://www.lemediatv.fr/articles/2020/politiques-de-lamphibiose-la-guerre-contre-les-virus-naura-pas-lieu-ACcrS8oIQsOuLQmmvfx2aQ

Or, un tel pas n'est pas nécessaire. Il l'est d'autant moins que nos relations effectives avec les virus en général sont moins belliqueuses et manichéennes (opposition bien/mal) que ne le laisse paraître la métaphore de la guerre. De même que nous découvrons depuis quelques années que nous sommes largement le résultat d'interactions multimillénaires avec des populations de bactéries qui peuplent notre organisme, intestins, peau, poumons, etc., de même, nos organismes sont constitués d'un nombre considérable de virus (« Nous avalons plus d'un milliard de virus chaque fois que nous allons nager », Carl Zimmer, biologiste[8]) qui remplissent parfois (comme les virus bactériophages Alexander Sulakvelidze, Zemphira Alavidze et J. Glenn Morris, « Bacteriophage Therapy », *Antimicrobial Agents and Chemotherapy*, vol. 45, nº 3, mars 2001, p. 649–659) des rôles essentiels au bon fonctionnement de l'organisme (voir Stéphane Biacchesi, Christophe Chevalier, Marie Galloux, Christelle Langevin, Ronan Le Goffic et Michel Brémont, Les virus : Ennemis ou alliés ?, Versailles, Quæ, coll. « Enjeux Sciences », 2017, 112 p.). Les virus ne nous sont donc pas « extérieurs ». Un organe aussi crucial pour la reproduction de la vie humaine que le placenta nécessite par exemple la production de syncytines. Or ces protéines sont codées par des gènes qui se sont intégrés dans l'ADN des ancêtres des mammifères à la suite d'infections virales[9]. En communiquant des brins de leur ADN à leurs organismes hôtes, certains virus ont ainsi joué, et jouent encore aujourd'hui, des fonctions essentielles dans l'évolution des espèces. Plus largement, une portion non négligeable de l'ADN humain s'est formé en empruntant certains de ses constituants à des virus. En s'adaptant à leur présence, en parvenant à contrôler dans certains cas leur pathogénicité, notre organisme a pu les mettre au service de ses fonctions vitales. Que faire de la métaphore guerrière sous cette perspective ?

Face au risque vital que SARS-COV-2 peut constituer dans certaines circonstances (liées à l'âge, à l'état de santé, à certains facteurs de prédisposition génétiques ou épigénétiques, socioéconomiques et géographiques, etc.) de nouvelles métaphores peuvent s'allier aux mesures mises en œuvre dans les pays touchés par la pandémie. Les stratégies dominantes aujourd'hui ne ressemblent d'ailleurs pas tellement à des actes de guerre, mais à des gestes de diplomatie et de prudence : limiter l'exposition au virus, réduire les échanges, se confiner, rechercher la distance qui sécurise, archiver ses contacts, communiquer sur les chaînes de propagation pour les endiguer, porter son masque, etc. Apprendre à vivre avec SARS-COV-2 appelle un autre art que celui de la guerre : l'art de la cohabitation, du voisinage, du contournement, de la juste distance, de la prévenance, etc. Comme le souligne Charlotte Grives :

> "Il incombe aux humains d'adapter leur organisation, c'est-à-dire la politique, au caractère [dynamique] de leurs relations avec les micro-organismes – relations changeantes, parfois pathogéniques, parfois non, selon des conditions qu'il faut comprendre. Depuis la découverte de la variolisation et du principe de la vaccination jusqu'aux stratégies actuelles pour gérer la pandémie du VIH, le problème est moins de lutter contre un ennemi invisible que d'apprendre à vivre, à devenir avec des entités biologiques qui ont leur mode d'existence propre. Il s'agit moins de se préparer au pire (même si les plans de préparation aux épidémies sont bien sûr nécessaires), que de prendre acte une fois pour toutes et tirer des conséquences de cette vie commune, de ces devenirs partagés. [...] »[10]

L'imaginaire de la guerre laisse ici place à revisiter nos relations avec la nature. De nombreuses publications d'anthropologues, de philosophes et historiens des sciences, voient en effet dans la crise actuelle une démonstration de plus en faveur de la nécessité d'une écologie politique réellement ambitieuse. Dans cette perspective, l'imaginaire de la guerre, les actions et les relations concrètes qu'il conditionne sont précisément ce dont il s'agit de se défaire au profit d'une nouvelle alliance entre les humains, avec les autres êtres et la nature. Ce dessaisissement de l'attitude et de l'imaginaire guerriers apparaît d'autant plus nécessaire qu'une fois levé le voile obscurcissant de la métaphore qui rend l'ennemi (le virus) « coupable » de tous les maux, la responsabilité de la crise actuelle se révèle en grande partie imputable à la victime elle-même (l'homme). On fait ainsi remarquer que « l'intensification de l'élevage industriel a démultiplié les risques de contamination, en plaçant des animaux consommés de façon intensive entre les réservoirs sauvages et humains[11]». On souligne la rapidité avec laquelle SARS-COV-2

[8] https://www.ouest-france.fr/sciences/sante-rarement-dangereux-les-virus-sont-partout-6785498

[9] A pair of co-opted retroviral envelope syncytin genes is required for formation of the two-layered murine placental syncytiotrophoblast. Dupressoir A, Vernochet C, Harper F, Guegan J, Dessen P, Pierron G, Heidmann T. 2011. Proc. Natl Acad. Sci. USA 108, E1164–E1173. (doi:10.1073/pnas. 1112304108);Chuong EB (2018) The placenta goes viral: Retroviruses control gene expression in pregnancy. PLoS Biol 16(10): e3000028

[10] https://www.lemediatv.fr/articles/2020/politiques-de-lamphibiose-la-guerre-contre-les-virus-naura-pas-lieu-ACcrS8oIQsOuLQmmvfx2aQ

[11] https://laviedesidees.fr/La-lecon-anthropologique-des-chauves-souris.html

s'est répandu sur la planète grâce à la globalisation des échanges économiques. On observe aujourd'hui que la toute grande majorité des victimes du COVID-19 y est prédisposée par des états de santé dégradés (maladies chroniques, affections respiratoires, obésité, tabagisme,...) en raison des habitudes de vie, des inégalités socioéconomiques et des pollutions industrielles. De ce point de vue, la cause première des victimes du COVID-19 n'est pas SARS-COV-2, ce sont les humains » (« l'agent pathogène dont la virulence terrible modifie les conditions d'existence de tous, « ce n'est pas du tout le virus, ce sont les humains » (Bruno Latour[12]) ou, pour être précis, les formes humaines d'organisation, de production, de consommation et de répartition des ressources qui se sont constituées ces derniers siècles dans l'irrespect du droit humain fondamental à la santé[13], des écosystèmes naturels, des barrières entre les espèces, etc.

Que l'humanité prenne conscience de sa responsabilité dans la crise actuelle est ainsi la première étape que les tenants du référentiel de nos relations avec la nature appellent de leurs vœux. La seconde étape qui s'en suit suppose, à l'instar de la responsabilité dans le réchauffement climatique, une transformation profonde des organisations sociales, économiques et politiques à l'échelle internationale. La métaphore d'une (ré)conciliation avec la nature se substituant à celle de la compétition ou de la lutte pour l'existence (paradigmes de base de l'économie classique et du *darwinisme social*), elle ouvre le champ des possibles à des actions en vue de réduire les nuisances industrielles, revoir nos théories et nos fonctionnements économiques, réduire les inégalités sociales, restaurer et refinancer nos systèmes de santé, bref réaligner nos formes de vie sur la hiérarchisation des valeurs à l'aune desquelles nous aspirons à vivre.

Comment de nouvelles technologies numériques employées dans le cadre de la crise actuelle, notamment à des fins de traçage, pourraient-elles trouver sens et se mettre en œuvre à l'aune d'une relecture de nos relations avec la nature ? Si la place et l'importance accordée aux technologies vertes (biomasse, éolien, solaire,...) dans un tel cadre de référence sont aisément concevables, les technologies numériques sont réputées particulièrement énergivores. Des études récentes montrent que l'évolution du numérique et de l'IA soulève effectivement des défis de fond en termes de soutenabilité (Strubell, Emma, Ananya Ganesh, and Andrew McCallum. "Energy and Policy Considerations for Deep Learning in NLP." *arXiv preprint arXiv:1906.02243* (2019)). De nombreuses recherches sont menées en ce sens dans l'objectif de développer des solutions numériques beaucoup plus vertes et durables. Leur usage doit aussi nécessairement s'inscrire dans le cadre plus large d'un Green Deal ou d'un plan de gouvernance démocratique de la crise, soumis à des critères rigoureux d'évaluation de l'impact environnemental.

Une utilisation réfléchie de l'IA associée au développement de *smart grids* a déjà montré que des progrès pouvaient être accomplis en matière d'économie d'énergie grâce aux technologies numériques. Par exemple, en recourant aux services de sa filiale DeepMind, Google a pu réduire la consommation énergétique de ses datacenters de 40 % en 2 ans. Des secteurs connus pour leur consommation énergétique peu économe (bâtiments, industries, transports...) commencent aussi à bénéficier de solutions intégrant des *smart grids* et de l'IA embarquée. Mais ces solutions n'en seront vraiment qu'à condition que les économies de ressources ou d'énergie obtenues grâce au développement d'une technologie plus verte ne soient pas partiellement ou complètement compensées par une augmentation, en retour, de la consommation énergétique (effet rebond). À côté des enjeux de production d'outils numériques responsables, deux facteurs essentiels de l'acceptabilité sociale des innovations technologiques à venir consisteront donc d'une part dans la capacité des concepteurs d'IA et solutions numériques à atteindre des objectifs d'économies de ressources, de recours aux énergies vertes et de durabilité, et d'autre part dans la mise en oeuvre de politiques environnementales contraignantes pour stimuler l'innovation technologique verte et réguler la consommation énergétique.

Si les solutions technologiques envisagées dans le présent rapport pour accompagner la sortie de crise COVID-19 ne sont pas directement conçues dans une visée de réduction de l'impact environnemental mais dans une visée de protection et d'aide à la reprise des activités sociales, économiques et culturelles, elles gagneront en légalité, en acceptabilité sociale et en avenir à intégrer l'éco-conception et la sobriété numérique au coeur de leur projet, et à s'insérer dans un processus plus large de transition énergétique et

[12] https://www.lemonde.fr/idees/article/2020/03/25/la-crise-sanitaire-incite-a-se-preparer-a-la-mutation-climatique_6034312_3232.html
[13] https://www.who.int/governance/eb/who_constitution_fr.pdf

environnementale. En mobilisant l'imaginaire et les ressources d'une approche plus écologique, elles pourraient aussi promouvoir une vision de l'outil technologique moins fondée sur la métaphore guerrière (combat contre la nature, contrôle populationnel, renseignement et propagande). Car elles s'ancreraient davantage dans l'horizon d'une écologie politique soucieuse d'une organisation intelligente de nos cohabitations et de nos relations entre êtres humains et non-humains.

4 LE RÉFÉRENTIEL DE LA SURVEILLANCE DE MASSE

S'il est difficile aujourd'hui de sous-estimer l'influence croissante de la métaphore de la (ré) conciliation avec la nature dans le contexte actuel du réchauffement climatique et de la reconnaissance de l'impact géologique de l'action humaine (Anthropocène), un autre imaginaire impacte dans la crise actuelle, sans doute plus directement et plus fortement que le précédent, la réception sociale des propositions technologiques, en particulier dans le domaine du traçage numérique. L'horizon imaginaire de la conciliation avec la nature offrait la possibilité de ne pas concevoir uniquement les technologies numériques sous l'angle de leur absence ou de leur "incompétence de jeunesse" (imaginaire des grandes épidémies passées), ou sous la perspective de l'arme de guerre, de la propagande et du renseignement (imaginaire de la guerre), mais comme des outils (plus ou moins verts et durables) de cohabitation et de protection (relative) en présence d'un agent non humain de passage. L'imaginaire des sociétés de la surveillance renoue pour sa part avec une préoccupation moins écologique, mais beaucoup plus sociale, juridico-éthique et politique. Dès l'apparition des premières propositions d'accompagnement numérique de la sortie de crise actuelle, de très nombreuses personnalités du monde académique et de la société civile ont pris part en effet au débat public pour mettre en garde contre la menace que constituait tout projet technologique de traçage numérique des mouvements de population pour les principes démocratiques, l'État de droit et les libertés fondamentales

L'objectivation de risques de dérives possibles et d'affaiblissement des droits et libertés démocratiques liés à un *recours irréfléchi* et mal encadré des technologies numériques, s'accompagne fréquemment de deux arguments bien connus des bioéthiciens, des logiciens et des philosophes : l'argument de la pente glissante et l'argument anti-solutionniste.

L'argument de la pente glissante est un type de raisonnement qui postule qu'à partir d'une prémisse donnée (la mise en place d'applications de traçage), il s'en suit avec une certaine probabilité (version honnête de l'argument), ou au contraire nécessairement (version malhonnête de l'argument), un ensemble d'effets conduisant vers une conclusion que personne ne souhaite (le remplacement d'un État démocratique par un État autoritaire et liberticide). Cet argument devient malhonnête lorsqu'il néglige qu'un ensemble de dispositifs démocratiques permettent de réduire sérieusement les risques de dérapages des technologies envisagées: cadres juridiques et éthiques stricts, contrôles externes, évaluation continue par les usagers, etc. Quant à **l'argument néo-luddiste**, il postule que tout projet de résolution d'un problème humain par une technologie est de nature solutionniste: il fétichiserait la solution technique au détriment de la considération d'une solution plus humaine, sociale, politique et éthique. Un tel argument est aussi problématique : il présuppose que l'outil technologique ne pourrait être un moyen parmi d'autres d'une solution plus globale, comme si l'un et l'autre s'excluaient d'emblée, ce qui est faux, bien évidemment.

L'extrait suivant donne un exemple explicite de recours aux arguments néo-luddiste et de la pente glissante, qui abondent dans un bon nombre de productions littéraires sur les dangers des technologies numériques dans la crise actuelle :

> "Even if [an] application is adopted by a part of [a] population on a voluntary basis, it is to be feared that the government could impose it more easily on the rest of the population or made compulsory, against its will [...]. Knowing that all security and liberticidal measures taken in times of "emergency" have never been questioned and no one is able to tell in advance how long [an] application will be deployed, once the application is deployed, it will be easier for the government to add enforcement functions (individual containment control) to it. Moreover, the application provides an incentive to subject one's body to constant surveillance, which will increase the social acceptability of other technologies, such as facial recognition or automated video surveillance [...] To conclude, these [proposed technological solutions to the current crisis]

> reinforce the blind belief in technology and surveillance as the main responses to health, ecological or economic crises, while on the contrary they divert attention away from solutions: scientific research, public service funding, etc. The use of an application whose objectives, techniques and conditions of use carry significant risks for societies and individual liberties, for probably poor (or even counter-productive) results, cannot be considered as an acceptable solution. The media, political time and budgets allocated for this purpose would be better used to inform and protect the population (and healthcare workers) by methods with proven effectiveness, such as the provision of masks, tests, medical care and equipment."[14]

Or, l'emploi de ces deux stratégies argumentatives n'est pas en soi nécessaire à toute alerte rationnelle fondée sur les risques possibles d'atteinte à l'État de droit ou aux libertés individuelles dans les cas où certaines procédures d'évaluation démocratique, éthique et juridique d'une technologie pourraient ne pas être appliquées (ou ne l'auraient pas été).Lorsqu'il devient hyperbolique, le recours à ces arguments peut pousser l'imaginaire de la surveillance de masse dans ses extrêmes, et substituer la « thèse conspirationniste » à l'oeuvre de raison, comme en témoigne cette lecture de la crise proposée le 26 février 2020 dans le journal italien *Il manifesto* par Giorgio Agamben, pourtant l'un des intellectuels réputés parmi les plus éclairés de ce siècle :

> « Il semblerait que, le terrorisme étant épuisé comme cause de mesures d'exception, l'invention d'une épidémie puisse offrir le prétexte idéal pour les étendre au-delà de toutes les limites. L'autre facteur, non moins inquiétant, est l'état de peur qui s'est manifestement répandu ces dernières années dans les consciences des individus et qui se traduit par un réel besoin d'états de panique collective, auquel l'épidémie offre une fois de plus le prétexte idéal. Ainsi, dans un cercle vicieux et pervers, la limitation de la liberté imposée par les gouvernements est acceptée au nom d'un désir de sécurité qui a été induit par ces mêmes gouvernements qui interviennent maintenant pour le satisfaire. »[15]

Agamben est un spécialiste reconnu en science et philosophie politique, pour avoir poursuivi à la suite de Walter Benjamin (1892-1940), Carl Schmitt (1888-1985) et Michel Foucault (1926-1984), la théorisation du concept d'"état d'exception". Dans ses travaux, à divers égards controversés), Schmitt s'est efforcé de défendre la légitimité de l'État à déclarer dans certaines circonstances la mise en place d'états d'exception. Aucune norme juridique, selon Schmitt, ne peut régir un cas d'urgence extrême mettant en péril une société dans son fonctionnement courant (guerre, catastrophe naturelle, épidémie...). Car dans une situation totalement anormale, l'application continue de la loi par des voies administratives et judiciaires normales ne permet pas de mettre en oeuvre les actions efficaces requises par la situation exceptionnelle. L'état d'exception est en ce sens, pour Schmitt, une disposition extra-légale que l'État peut solliciter au nom de sa souveraineté pour suspendre temporairement l'application de la Constitution quand l'ordre politique courant est menacé. Cette mesure permet de prendre des mesures extraordinaires, de passer outre l'avis du Parlement, de gouverner par ordonnances expresses, de suspendre des libertés publiques, etc.

[14] https://booksandideas.net/Tracing-Apps-to-Fight-COVID-19.html
[15] Agamben, 26 février 2020, https://ilmanifesto.it/lo-stato-deccezione-provocato-da-unemergenza-immotivata/

En commentant les travaux de Schmitt sur l'état d'exception, Giorgio Agamben pense l'état d'exception comme un dispositif juridique paradoxal qui permet d'inscrire dans le droit ce qui est extérieur à lui (c.-à-d. un pouvoir arbitraire, extra-légal) à travers la suspension de l'ordre juridique lui-même. Dans sa trilogie *Homo Sacer* (1997-2003), le philosophe italien associe à cette analyse la thèse de Walter Benjamin publiée en 1942 dans son ouvrage *Sur le concept d'histoire*, pour qui « l'état d'exception dans lequel nous vivons est en vérité la règle ». Agamben fait remarquer que les décrets et la régularisation d'états successifs d'exception avaient effectivement permis au parti national-socialiste, dans l'Allemagne démocratique des années 1930, d'imposer pas à pas un régime totalitaire au nom de la menace que constituaient, selon lui, certaines populations. Si le totalitarisme nazi fut défait au sortir de la guerre, Agemben affirme que les démocraties libérales restent néanmoins engagées depuis plus d'un siècle dans un processus de normalisation des états d'exception et d'indiscernabilité croissante de ces derniers avec le régime du droit commun. Le philosophe italien défend autrement dit l'idée que la subversion totalitaire de la démocratie allemande n'a pas été qu'un accident dramatique de l'histoire des démocraties occidentales. Le régime nazi fut une réalisation historique particulièrement radicale de la propension fondamentale des régimes démocratiques à tendre vers le totalitarisme par l'intégration, dans le droit commun, de pouvoirs non démocratiques qu'ils s'arrogent sous états d'exception. Lorsque ces états se succèdent, l'exception devient la norme. L'exemple de l'Allemagne nazie n'est donc pour Agamben qu'une manifestation (particulièrement détestable) parmi d'autres d'un « envers » totalitaire des régimes démocratiques parfois moins apparent au premier regard, mais qui trouve sa traduction sous diverses formes d'expressions historiques.

L'esprit de cette thèse d'Agamben déborde largement la seule pensée de ce dernier. Une partie non négligeable de la philosophie de la seconde moitié du XX^{e} siècle s'est attachée à mettre en garde contre les risques des dérives totalitaires des sociétés occidentales, caractérisées dans leurs formes les plus courantes par un accroissement du pouvoir de contrôle et de surveillance des individus que s'accordent les États. Quantité de chercheurs, essayistes, journalistes et analystes de l'actualité recourent au filtre de l'imaginaire de la surveillance de masse et de la théorie des états d'exception permanents, pour interpréter nombre d'événements politiques et de faits de société survenus ces dernières décennies comme autant de traces, au sein des États de droit, de velléités totalitaires, anti-démocratiques et liberticides: création de zones permanentes de non-droit dans ou par des pays démocratiques (Guantanamo, camps de réfugiés politiques, climatiques...), surveillance de masses des citoyens à leur insu (écoutes de la NSA et affaire Snowden), poursuites pénales contre des lanceurs d'alerte souhaitant préserver l'État de droit de ses dérives antidémocratiques, prolongements, plus que de raison, d'états d'urgence antiterroristes, normalisation d'ordonnances et de pouvoirs exécutifs temporairement légitimes en situation d'état d'exception, mais non nécessaires, disproportionnés et susceptibles d'atteindre aux droits et libertés fondamentales dans le régime du droit commun, etc. La crise actuelle liée à SARS-COV-2 et la perspective d'une légitimation par les États du recours à des technologies de traçage numérique des mouvements de population ou des individus, n'échappe pas non plus au contexte imaginaire d'arrière-plan de la surveillance de masse qui voit, dans chacun de ces phénomènes, une démonstration de la validité de la thèse de l'envers ou du devenir totalitaire des démocraties occidentales.

L'interprétation devient même extrême lorsqu'elle prend, comme dans les positions d'Agamben sur l'épidémie de COVID-19, un tour conspirationniste. Puisant dans les ressources les plus obscures de l'imaginaire de la surveillance de masse, Agamben considère en effet que l'épidémie constitue une "invention" politique. Non qu'il s'agisse, pour le philosophe italien, de nier l'existence de SARS-COV-2 et son oeuvre épidémique, mais d'affirmer que la perception de sa dangerosité est globalement surestimée et constitue, en ce sens, une forme de construction politique. Produit d'un processus anonyme (sans sujet clairement identifiable à la manœuvre), Agamben fait ensuite remarquer que cette construction politique de la perception de l'épidémie de COVID-19 n'est pas sans inconséquence. Elle permet de justifier, après l'essoufflement du mobile antiterroriste, la promulgation d'un nouvel état d'exception - l'état d'urgence sanitaire. À la lumière de sa théorie des dérives totalitaires des sociétés démocratiques, Agamben soutient alors que la finalité d'un tel décret ne s'inscrit pas fondamentalement (quoiqu'en apparence) dans une visée de santé

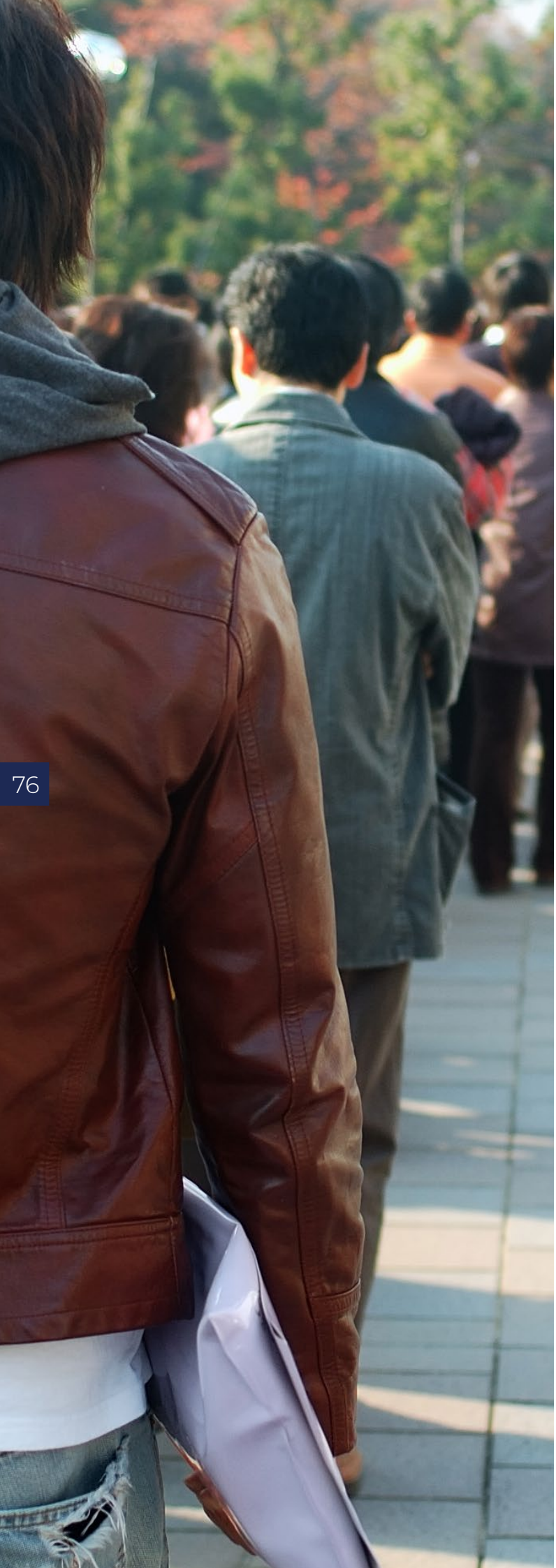
publique (imaginaire du soin), mais dans la profonde propension totalitaire des régimes démocratiques à réduire les libertés et accroître le pouvoir de surveillance des États sur les citoyens et leur vie privée. Sans référence aux démocraties asiatiques, Agamben voit en ce sens dans l'intérêt manifeste des pays européens pour l'efficacité des politiques chinoises de gestion de la crise sanitaire, un aveu de jalousie à peine masqué pour les moyens et capacités qu'un pays autoritaire, non démocratique et liberticide comme la Chine peut mettre en oeuvre pour le contrôle d'une population.

Une telle interprétation constructiviste et conspirationniste de la pandémie de COVID-19, de l'état d'urgence sanitaire, et de la fonction qu'y tiendraient les technologies de traçage numérique, est évidemment problématique et réductrice à divers égards. Elle l'est par rapport à la réalité des faits, de la maladie et de ses victimes ; elle pèche par son « déni spéculatif » de la force des mécanismes institutionnels, éthiques, juridiques et politiques de protection des droits et libertés fondamentales dont nos démocraties se sont dotées depuis la Seconde Guerre mondiale pour se protéger des dérives idéologiques toujours possibles qui pourraient pervertir leur nature. Elle constitue enfin une forme d'aveu d'impuissance en postulant l'existence d'un processus anonyme qui s'imposerait nécessairement à nos démocraties, nos libertés et nos histoires, et sur lequel l'intelligence humaine, l'exercice du jugement éthique, les résistances du droit et l'action collective n'auraient aucune prise. En dépit de la prudence justifiée avec laquelle il convient donc d'accueillir les mises en garde contre les risques de dérives totalitaires de nos États démocratiques, une attitude naïve de la société civile face aux décisions du pouvoir dans la crise actuelle serait à l'inverse tout aussi problématique. Dans les pays où la démocratie est affaiblie depuis de nombreuses années, comme le montre le cas de la Hongrie, la situation présente peut servir de mobile pour renforcer la concentration de tous les pouvoirs entre les mains de l'exécutif[16].

Si l'imaginaire conspirationniste peut contribuer à maintenir la société civile vigilante et en alerte contre les risques éventuels de dérives autoritaires de certains États, et si par ailleurs la crainte de la propension des États de droit au totalitarisme demeure vivante en vertu des symboles qu'elle sollicite et des souvenirs qu'ils éveillent eu égard aux épisodes les plus sombres de l'Histoire, l'imaginaire de la surveillance et des technologies de traçage n'est pas seulement hanté des événements les plus obscurs de l'histoire du XXe siècle. Certes, les régimes totalitaires ont toujours recouru abondamment à des outils de traçage pour obtenir du renseignement sur les individus et les populations, réprimer toute velléité d'opposition politique et imposer un modèle de comportement et de pensée conforme au pouvoir. Il est donc normal que l'évocation de cette réalité, toujours d'actualité dans certains pays aujourd'hui, génère une méfiance sociale *a priori* par rapport aux technologies de traçage numérique à l'échelle individuelle ou populationnelle. Pourtant, ce réflexe culturel opère une réduction du sens de la surveillance et des technologies de traçage numérique, pour n'en retenir que leur portée négative. Or, la surveillance et le traçage numérique sont aussi porteurs de positivité et sources de biens souhaitables.

Il convient tout d'abord de rappeler que les technologies de traçage numérique ne conduisent pas nécessairement à l'autoritarisme ou au totalitarisme. Combien de personnes en danger, coincées en montagne ou perdues dans un environnement méconnu, n'ont pas été secourues grâce au bornage téléphonique ou l'activation du GPS de leur smartphone ? Combien de crimes de diverses natures n'ont-ils pu être déjoués grâce au renseignement numérique ? Dans certaines configurations, le traçage numérique offre des garanties de protection et de secours sans équivalent dans l'Histoire. Sous certaines conditions prévues par la loi, les possibilités médicales de suivi des patients et de leurs paramètres physiologiques offrent également des perspectives thérapeutiques formidables dans le champ de la médecine personnalisée. Les outils de traçage numérique donnent à de très nombreux sportifs la possibilité de mesurer leurs performances en temps réel, de programmer des entrainements de course adaptés, d'évaluer leur progression sur la base d'indicateurs bio et physiologiques de plus en plus précis. Dans le domaine du marketing, le traçage numérique permet aussi de proposer aux individus des services et des produits plus personnalisés, mieux adaptés à leur situation et leur parcours de vie. À l'échelle d'une ville, il offre la possibilité d'optimiser l'organisation des infrastructures en fonction de l'analyse des déplacements de foules, du trafic routier, etc. Mais il est vrai que le traçage numérique comporte aussi de nombreuses dérives possibles : perte de l'intimité et de la vie privée, divulgation des données personnelles, utilisation non éthique de

[16] https://www.lawfareblog.com/understanding-hungarys-authoritarian-response-pandemic



données sensibles à son insu, commercialisation des données de santé, vol de données, piratage des outils numériques, stigmatisation de certaines catégories de population, abus de pouvoir des autorités publiques, etc.

Au regard de ces différents exemples, les technologies de traçage numérique sont donc capables du meilleur comme du pire, et il n'existe pas de lien de consécution *nécessaire* qui les destinerait à un avenir totalitaire. Il en est de même pour la surveillance, qui répond en soi à de profondes attentes sociales. Il importe ici de revenir au sens même du concept et à ses usages légitimes.

Avant d'être détournée de ses fins premières par les totalitarismes du siècle dernier, la surveillance s'est instituée au sens moderne du terme entre les XVI^{e} et XIX^{e} siècles. Dans ses travaux (Surveiller et punir, 1975), Michel Foucault fait remarquer que ce n'est pas un hasard si l'apparition du terme dans la langue française concorde avec la naissance de l'État de droit. « Surveiller » s'est forgé au XVI^{e} siècle à partir du verbe « veiller » qui signifie « rester en éveil (pour intervenir en cas de besoin) », « rester vigilant », et du préfixe « sur » qui indique l'excès ou la supériorité. L'usage du verbe s'est ensuite généralisé aux XVIII^{e} et XIX^{e} siècles, donnant naissance au mot « surveillance ». Or, dans la tradition contractualiste (théories du contrat social) qui fonde nos démocraties libérales, la surveillance constitue au sens positif du terme (*veiller sur),* un moyen légitime d'assurer l'ordre public et un devoir confié aux États qui se doivent de garantir aux citoyens leur protection et les meilleures conditions possibles d'exercice de leurs droits et libertés fondamentales. Foucault montrera dans ses travaux qu'il existe par ailleurs un lien intime entre la surveillance et la discipline. Le contrôle populationnel, tout autant que la sanction, induit la genèse de comportements sociaux prévisibles qui sont nécessaires au maintien de l'ordre public et de la productivité économique (pour la plupart des opérations répétitives) d'une nation.

À fin constante, les moyens de la surveillance et de la discipline employés par les États vont cependant évoluer au cours du temps. Si avant l'âge classique, la surveillance des États ne pouvait s'exercer qu'à faible amplitude humaine et technique (ressources humaines policières, administratives), la discipline des corps s'obtenant dès lors par l'intimidation, la punition publique, l'exclusion des

indésirables et la mise à mort des contrevenants à l'ordre public, Foucault montre que ces politiques sanglantes ne vont cesser par la suite de s'atténuer sans pour autant que l'ordre public en soit affecté. Comment comprendre ce phénomène, sinon par une évolution parallèle des moyens de surveillance des populations ? À l'ère de l'âge classique, Foucault voit en effet se succéder une ère nouvelle, l'ère de la biopolitique. Cette nouvelle configuration historique des sociétés se traduit dans une alliance inédite entre la politique, l'économie et la médecine, où la surveillance légitime exercée par l'État, désormais plus diffuse, moins repérable, moins concentrée, moins maîtrisée, plus déléguée et moins dépendante de la seule puissance publique, n'en devient cependant que plus efficace quant à ses effets sociaux. Foucault illustre cette nouvelle forme de surveillance diffuse des sociétés à l'ère de la biopolitique par la célèbre figure du *Panopticon* (qui traduit en grec l'idée de voir partout). Ce projet de bâtiment pénitentiaire (qui ne verra jamais le jour) fut architecturalement conçu sur plan par Jeremy Bentham (1748-1832), de telle façon que chaque prisonnier s'y sache toujours potentiellement visible pour ses surveillants sans jamais avoir la certitude d'être effectivement observé. Une telle incertitude conduit les individus à s'auto-discipliner en fonction des attendus du système pénitencier, sans que ses dirigeants aient plus à investir outre mesure en ressources humaines de surveillance et de répression sociale :

> « Celui qui est soumis à un champ de visibilité, et qui le sait, reprend à son compte les contraintes du pouvoir ; il les fait jouer spontanément sur lui-même ; il inscrit en soi le rapport de pouvoir dans lequel il joue simultanément les deux rôles ; il devient le principe de son propre assujettissement. Du fait même le pouvoir externe, lui, peut s'alléger de ses pesanteurs physiques ; il tend à l'incorporel ; et plus il se rapproche de cette limite, plus ces effets sont constants, profonds, acquis une fois pour toutes, incessamment reconduits : perpétuelle victoire qui évite tout affrontement physique et qui est toujours jouée d'avance. » (M. Foucault, *Surveiller et punir*)

Le panoptisme constitue ainsi pour Foucault la métaphore d'un système de surveillance et de discipline sociétal intériorisé par les individus, qui caractérise les sociétés à l'ère de la biopolitique. Le philosophe français voit ce système comme une émergence des interactions entre la politique, l'économie et la biomédecine qui responsabilise les individus à l'ère du capitalisme et du (néo) libéralisme. La tâche leur est en effet confiée d'exercer leur autonomie pour s'ordonner par eux-mêmes, en toute « liberté », aux finalités des lois du marché et de l'auto-régulation des sociétés démocratiques. L'indépendance de l'individu n'est bien sûr que relative (c'est un leurre) : dans les sociétés démocratiques libérales, la liberté de chacun demeure soumise à une surveillance anonyme (système panoptique) et intériorisée (psychiquement) qui conditionne les comportements individuels aux finalités de l'ordre public, des lois du marché et d'une quête de santé indéfinie.

Cette histoire foucaldienne des mutations des formes de la surveillance des États de droit ne contient pas de jugement de valeur (Foucault ne se positionne pas moralement par rapport au processus historique qu'il analyse). Comme nous l'avons souligné, la surveillance est un moyen essentiel des États pour garantir l'ordre social, protéger les individus, et rendre possible l'exercice des droits et libertés individuelles. La démarche de Foucault montre comment cette surveillance, ainsi que les disciplines qu'elle induit, se sont transformées au cours du temps. Objectives et repérables, publiquement violentes, la surveillance s'est progressivement étendue et anonymisée. Les disciplines se sont psychiquement intériorisées à l'intime du sujet libéral. La sanction sanglante des transgressions des disciplines sociales, infligée autrefois par la puissance publique, s'est éloignée de l'échafaud des places publiques pour laisser place à d'autres mécanismes punitifs, plus socialisés ou intériorisés (perte de réputation sociale, culpabilité, névroses et maladies psychiques).

Si Foucault ne l'a pas connue de son vivant, on peut soutenir que la numérisphère constitue l'une des technologies les plus abouties du panoptisme des sociétés démocratiques libérales. La numérisphère désigne l'omniprésence du Web, des outils numériques et de connectivité dans nos vies, à l'image d'une seconde atmosphère, mais dont l'oxygène que nous respirons se compose d'algorithmes et de données. Nous inspirons continuellement des données par l'usage de nos smartphones, ordinateurs et objets connectés, nous en expirons tout autant, laissant dans la numérisphère, la plupart du temps à notre insu, des traces identifiables, personnalisées, de nos passages. Or, à l'instar de l'atmosphère et des conditions d'observation et de mesure des variations de pressions et de températures que nécessite la

météorologie pour ses prédictions, la numérisphère est truffée de myriades de capteurs d'informations, issus d'instances publiques ou privées, qui peuvent y observer, à l'échelle individuelle ou populationnelle, les tendances et les variations comportementales à des fins de surveillance et de prédiction diverses.

Cependant, si nos données respirées sont continuellement monitorées par les météorologistes de la numérisphère, la métaphore atmosphérique s'arrête là, car si les outils de la météorologie n'ont pas d'influence sur le temps qu'il fait, les moyens de la numérisphère influencent quant à eux profondément les comportements des individus, soit à des fins d'ordre public pour les États (renseignement, contrôle), soit à des fins économiques (prédiction des besoins de consommation, établissement de profils clients, conditionnement des préférences individuelles) ou à des fins de santé (traçage des données bio- et physiologiques, suivi de recommandations thérapeutiques, etc.). La numérisphère constitue en ce sens un espace panoptique de visibilité, où les individus, se sachant potentiellement visibles à tout instant par des entités anonymes (publiques ou privées) dont l'activité « numérisphérique » est particulièrement discrète quoique omniprésente, intériorisent et mettent en œuvre une discipline de conduite qui correspond aux attentes des grandes institutions des sociétés démocratiques libérales et de la numérisphère à l'ère de la biopolitique : l'État, l'Économie, la Biomédecine.

Cette réalité composite, multipartite de la numérisphère, est bien décrite par Jean-Gabriel Ganascia, professeur d'informatique à la faculté des sciences de Paris Sorbonne Université :

> « Sans approfondir l'analyse spécifique du savoir produit par les dispositifs et les technologies de surveillance dans les sociétés contemporaines, notons seulement qu'il s'agit d'un savoir disséminé, c'est-à-dire d'un savoir produit par un très grand nombre d'acteurs (l'État, les entreprises, les individus, etc.), pour des motifs extrêmement divers (des objectifs policiers, économiques, statistiques, commerciaux, etc.). D'autre part, en dépit de cette dissémination, il se dégage de cette « surveillance » un objectif général qui n'est généralement pas directement coercitif, mais qui traduit bien plutôt [de multiples stratégies d'influence]. [...] Cette surveillance permanente, proactive et généralisée est enfin largement *décentralisée*, notamment en raison de la multiplication des acteurs qui, pour des objectifs extrêmement divers, récoltent et traitent des données personnelles, non sans offrir incidemment aux autorités publiques elles-mêmes de nouveaux instruments de collecte de l'information – comme le montre, en France, le fait que certains acteurs privés sont légalement obligés de conserver certaines données collectées pendant une durée déterminée ; de même, les compagnies aériennes, les grandes entreprises du Web, ou encore les banques, sont toujours davantage invitées à collaborer avec les services étatiques en charge des questions de sécurité, notamment dans le cadre de la lutte anti-terroriste. »[17]

Ainsi, les acteurs étatiques et économiques auxquels s'ajoutent, avec une intensité croissante ces dernières années, les grands acteurs publics et privés de la santé, constituent l'étoffe ou la toile de fond de la surveillance numérisphérique. Foucault soulignait déjà à son époque l'alliance entre ces trois pôles public, économique et médical qui caractérise l'ère de la biopolitique. Dans la numérisphère, ce partenariat se traduit par un développement continu des interactions et des partages d'informations de traçage entre les acteurs publics, économiques et de santé, qui y trouvent chacun des intérêts bénéfiques au regard des missions qui relèvent de leurs compétences (maintien de l'ordre, contrôle administratif, performance économique, profilage commercial, personnalisation des services, suivi de santé, identification des risques de santé, suivi médical des patients à domicile ou dans leurs activités quotidiennes...). Ces échanges de données demandent une vigilance démocratique de tout instant quant aux risques d'atteintes à la protection de la vie privée, des droits et des libertés fondamentales des citoyens. Elles font donc l'objet depuis plusieurs années de réglementations éthiques et juridiques de plus en plus exigeantes et robustes qui permettent d'apporter un cadre numérique sécurisant et protecteur des valeurs démocratiques et des libertés individuelles.

L'analyse foucaldienne, associée au champ de la numérisphère, montre l'omniprésence de la surveillance et son acceptation sociale au nom de la protection, de la sécurité et du bien-être qui sont classiquement attendus de l'État (contrat social), et

[17] https://books.openedition.org/editionscnrs/20197?format=reader

étendus, à l'ère de la biopolitique, à l'Économie et la Biomédecine. La surveillance est un fait politique et sociétal dont la numérisphère et les technologies de traçage font partie des moyens d'expression par excellence. Elle n'est pas en soi négative ni immédiatement attentatoire à la liberté ou la vie des individus, au contraire, dans ses usages légitimes, elle constitue un moyen de protection légitime de la liberté et de la vie, au service du bien individuel et public. Il est toutefois vrai que dans ses utilisations illicites, la surveillance et ses techniques peuvent causer du tort aux individus et au bien commun. La surveillance, la numérisphère et le traçage numérique ne peuvent en ce sens être jugés a priori, sans un examen attentif des enjeux éthiques que soulève chacun de leur point d'application.

Au regard de l'ensemble des développements qui précèdent, il n'est donc pas étonnant que l'imaginaire de la surveillance de masse et les technologies de traçage numérique contemporaines éveillent inévitablement des réactions contradictoires et ambivalentes dans le cadre de la crise actuelle. Les technologies de traçage numérique sont en effet capables du meilleur comme du pire. Néanmoins, comme nous l'avons montré, il n'existe pas de lien de consécution nécessaire qui les destinerait à un avenir néfaste pour l'humanité. Un encadrement politique, législatif et éthique soucieux de la protection des valeurs démocratiques et des libertés fondamentales peut constituer une protection efficace contre les risques de mésusage de la numérisphère et des technologies de traçage numérique, afin que leurs inconvénients soient minimisés, et leurs bénéfices maximisés.

Dans la situation de crise actuelle, qui demande une analyse et un jugement particuliers adaptés à la réalité présente, nous avons besoin d'un contrat social explicite et public qui garantisse que nous nous orientons davantage vers l'amélioration des aspects bénéfiques de la « surveillance » pour les individus et le public (par exemple, le suivi des maladies, la promotion de comportements au service du bien commun, etc.). Les citoyens doivent être capables de comprendre à la fois l'étendue et les limites de la surveillance. Les acteurs étatiques et les entreprises doivent accepter que leurs activités de surveillance (de veille sur) soient encadrées par des normes éthiques et juridiques qui reflètent les attentes de la société civile. Même si au regard de buts poursuivis comme légitimes, l'illimitation de certaines activités de surveillance optimiserait leur efficacité fonctionnelle en démocratie, la fin ne justifie pas tous les moyens.

5 LE RÉFÉRENTIEL DU SOIN

Le contrat social spécifique appelé par le contexte actuel, doit s'inscrire dans un ensemble de pratiques sociales, politiques et économiques orientées par une visée de fond qui doit être très largement partagée au sein de la société civile. Cette visée se doit d'être aussi pleinement ajustée à la réalité de la situation de crise actuelle et aux besoins sociaux qui pourraient s'exprimer dans ses prolongements imprévisibles. Ce n'est en effet qu'en référence à cette visée commune et son accordance avec la réalité de la crise traversée, que la fonction, la place et les principes d'usage des technologies numériques d'aide à la sortie de crise doivent être déterminés dans leurs possibilités et leurs limites infranchissables. Or, quelle est cette visée ?

L'innovation technologique, la numérisphère et l'intelligence artificielle ne sont pas – sauf aliénation – des fins en soi, mais des moyens au service de la réalisation de nos fins humaines. Si celles-ci sont en général très diverses, parfois conflictuelles, la situation actuelle de sortie de confinement et d'exposition possible à SARS-COV-2 fait figure d'un englobant. Elle définit une situation à risque spécifique qui concerne le vécu de tout un chacun dans la reprise de sa vie courante. Pour reprendre un concept proposé par Marcel Mauss dans son *Essai sur le don*, nous sommes ici en présence d'un « fait social total » qui affecte la totalité de la société et de ses institutions, et inspire à toutes et tous une même visée ou « orientation » partagée. Dans le cas qui nous occupe, nous voulons tous en finir avec la pandémie, avec les restrictions qu'elle nous impose, avec leurs conséquences sociales, économiques et culturelles. Nous sommes donc aussi tous concernés par les moyens pour y parvenir. C'est bien pourquoi nous avons besoin d'un contrat social explicite : nous demandons que le choix de ces moyens se fasse de façon transparente, en dialogue avec toutes les parties prenantes de la société civile, et dans l'objectif de la sortie de crise. Pour le dire autrement : face au fait social total que constituent l'expérience de la pandémie et ses conséquences, toutes les parties prenantes de la société civile ont besoin d'être (r)assurées (sur le fait) que les

moyens – notamment technologiques – qui seront envisagés et implémentés pour accompagner la sortie de la crise seront bien au service de cette visée universellement partagée – et non au service de fins particulières. Nos sociétés démocratiques attendent donc des États qu'ils soutiennent, avec l'ensemble des parties prenantes (publiques et privées), l'élaboration de cadres de gouvernance et de régulation à même de garantir l'adéquation des moyens envisagés pour la sortie de crise au bien visé par toutes et tous. De quelle nature sont cette visée et ce bien communs ? De nombreux référentiels, nous l'avons vu, sont sollicités dans la crise pour lui donner des sens divers et proposer des pistes d'action correspondant aux imaginaires mobilisés. Certains de ces référentiels ont pu paraître plus adéquats que d'autres à la situation de crise. Mais la visée qui mobilise la grande majorité des énergies et espoirs de nos concitoyens dans la réalité présente, demeure néanmoins d'une autre nature, car nous ne sommes pas réellement en guerre, confrontés à un enjeu de défense où l'ennemi est extérieur à la Nation, ou met en danger la stabilité de l'État. Nous ne sommes pas non plus dans un état d'urgence antiterroriste, face à un enjeu de sécurité où l'ennemi est identifiable à certaines catégories spécifiques de la population, ou à certains profils. Nous sommes plutôt dans une situation où chacun est potentiellement un risque et un soutien pour autrui, où chacun est appelé à la responsabilité pour soi et pour autrui. Nos préoccupations présentes, liées au « fait social total » que nous expérimentons actuellement, n'ont pas été non plus suscitées par des pratiques de surveillance inacceptables (affaire Snowden, Cambridge Analytica…) mais par l'expansion d'une pandémie et ses multiples effets sociaux, économiques, politiques. Nous ne sommes pas non plus mobilisés en première ligne par des pourparlers avec la nature en vue d'une nouvelle alliance, comme dans le cas de la problématique du changement climatique.

Si le « fait social total » actuel qui affecte tout un chacun, en particulier dans les sociétés occidentales les plus touchées, convoque un autre imaginaire et un autre registre d'actions collectives que ceux qui viennent d'être rappelés, il ne saurait être non plus univoquement assimilé aux grandes épidémies meurtrières de peste ou de grippe espagnole qui ont décimé des pans entiers de populations à leurs époques respectives, ni au danger que constitue, par exemple, le virus Ebola, avec un taux de mortalité autrement supérieur à SARS-Cov-2 (quoique moins susceptible d'atteindre l'échelle d'une pandémie). Cependant, la situation actuelle appartient bien à une même classe de situations que ces derniers cas : nous sommes bien dans un enjeu de santé publique qui met en jeu la préservation d'un bien commun, la santé, que nous cherchons à préserver pour le plus grand nombre possible d'entre nos concitoyens, en particulier celles et ceux d'entre nous qui sont les plus exposés aux morbidités de la COVID-19. Si l'état d'urgence sanitaire entretient des similitudes avec d'autres états d'exception dans les moyens sollicités, la fin est donc très différente, et l'esprit des mesures l'est aussi. En prendre conscience est essentiel pour ne pas se tromper de discours, d'horizon imaginaire, et de visée. Confrontés avec la pandémie à un enjeu de santé publique, nous ne sommes pas en guerre, nous sommes *en care*, et *en besoin de care* avant tout autre référentiel mobilisable, avant tout registre d'action parallèle, compatible ou complémentaire avec nos besoins dans la situation présente.

Le référentiel du *care* manifesté n'est pas réductible à l'univers médical et son acception clinique. Ces derniers en font toutefois bien évidemment partie et occupent dans la gestion de la pandémie un rôle essentiel. La première image que nous conserverons en effet de la période du confinement traversée sera celle de nos hôpitaux et de nos soignants, mobilisés aux limites extrêmes de leurs capacités par l'arrivée massive en soins intensifs des victimes les plus touchées par la maladie. C'est le risque d'explosion de nos structures hospitalières, face au nombre de cas estimés sans l'intervention de l'État, qui a d'ailleurs justifié la mise en confinement, partiel (comme en Suède ou aux Pays-Bas par exemple) ou total (comme en France, en Italie et dans de nombreux pays) des populations dans nos sociétés démocratiques. La situation prolongée du confinement et le risque épidémique ont mis en évidence à la fois la valeur inestimable et l'importance fondamentale de nos services de santé, de nos soignantes et soignants, mais ils ont aussi révélé à quel point ces services souffraient depuis de nombreuses années de politiques publiques de réduction successives de leurs financements, de leurs moyens et de leurs infrastructures.

Toutefois, cette prise de conscience de la profonde exposition de nos sociétés au risque épidémique et leur dépendance aux structures de santé, n'est qu'un reflet d'une prise de conscience beaucoup plus large qui s'opère avec le confinement : tout un chacun a pu y faire l'expérience que la continuation de sa vie et de ses échanges (à distance) avec autrui, dépendait d'un ensemble d'acteurs en général invisibles et

peu valorisés socioéconomiquement dans nos sociétés : manutentionnaires, caissières et caissiers, transporteurs, factrices et facteurs, techniciennes et techniciens de surface, agentes et agents de nettoyage, agricultrices et agriculteurs, gestionnaires de réseaux, etc. Les inégalités de traitement (salaires, conditions de travail, etc.) et l'exposition aux risques de santé entre ces métiers du *care* et ceux qui, en général, furent confinés ou sont les plus valorisés en société n'en sont aussi apparues que plus criantes. Aux antipodes du fantasme néolibéral du « *self made man* », nous avons pris conscience que nos vies dépendaient fondamentalement de l'engagement et du courage quotidien de nombre de nos semblables qui oeuvrent silencieusement, avec une constance remarquable, au maintien des conditions matérielles de base de nos vies fondamentalement vulnérables. Pourquoi de telles activités sont-elles si peu reconnues et valorisées dans nos sociétés démocratiques, quand elles sont si importantes et essentielles à la tenue de notre monde ? Les images du confinement n'ont rendu que plus visibles et choquantes de telles inégalités, quand le confort et la qualité de vie manifeste des uns (transgressant parfois les mesures d'exception pour rejoindre leur résidence secondaire en bord de mer ou en campagne) contrastaient avec l'insalubrité des bâtiments, la promiscuité et la pauvreté des conditions de survie d'autres vies confinées.

Ce constat de nos vulnérabilités partagées mais aussi des inégalités profondes de santé (niveau d'exposition au risque) et de salaire mises en évidence dans la crise, rejoignent des analyses formulées depuis deux décennies par les *éthiques du care*. De même, alors que la question du soin apparaît plus que jamais essentielle en pleine crise, sa prise en compte comme réponse politique nécessaire à nos vulnérabilités et nos interdépendances, est au cœur de cette littérature.

Les penseurs du *care* s'opposent aux conceptions modernes de l'individu « auto-entrepreneur » de sa vie, qui l'isolent de ses réseaux de dépendance et des millions d'actes de soin de diverses natures (soin parental, éducatif, social,...) dont tout un chacun bénéficie au cours de sa vie pour s'épanouir, développer ses capacités, s'affirmer comme sujet et constituer à son tour un soutien pour d'autres sujets. Une attention renouvelée aux activités du *care* dans nos vies nous montre en effet que ces dernières y sont omniprésentes, et que la réussite socioéconomique des uns n'est une réalité que parce que d'autres en assurent les conditions invisibles. Sans agentes et agents de ménage, de nettoyage, sans soutien aux tâches de secrétariat et d'administration, sans suivi de santé, sans support logistique, sans éboueuses et éboueurs, sans effectifs engagés dans l'entretien des espaces urbains, des moyens de consommation, de production et de communication, sans nourriture sociale et affective (familles, amis,...), etc., le mythe de l'individu « auto-suffisant » s'écroulerait. Car c'est bien d'une magistrale fiction dont il s'agit ici. En réalité, il n'existe pas d'être humain qui ne soit continûment dépendant au cours de sa vie d'un réseau d'attentions et d'actes de soins de multiples natures qui rendent son style et son mode de vie possibles en société. Les réussites « individuelles » ne sont que la partie visible d'un iceberg de gestes de *care* immergés dans un océan d'oubli. Entendons-nous bien : les éthiques du care ne contestent pas en soi les valeurs libérales comme l'autonomie, la liberté

d'entreprendre, le mérite par l'effort individuel, le refus du naturalisme (déterminismes de classe, reproductions sociales…), etc. Elles soulignent que ces valeurs ne peuvent être considérées indépendamment des relations innombrables de soin qui rendent possibles l'autonomie, l'entreprise, l'effort individuel, les changements de trajectoire sociale…

À l'anthropologie fictionnelle d'un sujet indépendant, les éthiques du care substituent donc une anthropologie relationnelle, fondée sur la vulnérabilité et l'interdépendance des sujets. Une telle anthropologie du soin s'accompagne bien évidemment de recommandations sociales, politiques et économiques, à commencer par une conséquence immédiate des développements qui précèdent.

Les penseurs du care soutiennent que les tâches du soin, en général occultées et peu valorisées, doivent être davantage reconnues comme condition *sine qua non* de l'activité économique. Il ne peut exister de libéralisme (et *a fortiori* de néolibéralisme) sans une réelle considération (et valorisation) des activités du soin.

Il revient ici à l'État d'assurer sa mission de redistribution équitable des ressources, et aux entreprises de traduire cette prise de conscience dans des politiques internes qui honoreront leur responsabilité sociétale. Car les métiers du soin ne sont pas moins importants ni moins valorisables que les autres. Ils comportent une attention à autrui et au monde qui devrait servir de modèle pour toute profession confondue.

Les penseurs du *care* recommandent de dépasser également d'autres obstacles à la reconnaissance du soin dans nos cartes mentales.

Le premier d'entre eux concerne une division classique entre les pratiques du soin et l'économie, la sphère domestique et la vie publique. Nous avons en effet hérité de schèmes de pensée qui nous représentent le soin comme une disposition et une pratique qui ne concerneraient que certains types d'activités : les soins parentaux, l'entretien de la maison, le soutien affectif, le soin médical, les soins de fins de vie, etc. Or, ces activités sont en général destinées à des sujets dépendants (enfants, malades, personnes âgées ou handicapées…) et ont généralement cours dans des espaces privés, des lieux cliniques ou des relations relevant de l'intimité de la vie familiale. Cette position « géographique » du soin le situe ainsi à distance des espaces publics où s'exercent l'activité économique et la vie politique. Celles-ci apparaissent dès lors comme dénuées de toute relation de soin, semblant former par contraste un espace tout indiqué pour des sujets indépendants, mus par des rationalités de marché.

Ce tableau de contrastes est parodique, mais il traduit une forme d'imaginaire culturel du soin qui influence la façon dont nous nous représentons le monde. Pour les éthiques du care, nous l'avons souligné, cette représentation n'est pas juste. Nous dépendons toutes et tous des attentions et du soin d'un grand nombre d'acteurs privés et publics. L'expérience du confinement le confirme encore : les fermetures d'écoles, les annulations d'événements publics, la subversion des espaces domestiques par les politiques du travail à domicile, associées aux rappels constants de se laver les mains, de couvrir sa toux et de rester à la maison dès l'apparition de symptômes suspects, ont fait voler en éclat, si besoin était, nos divisions mentales d'avant la crise. En nous rappelant notre vulnérabilité et notre interdépendance fondamentales, la pandémie nous appelle à un « prendre soin » général qui traverse non seulement les frontières du privé et du public, mais qui interpelle aussi profondément la façon dont nous mènerons à l'avenir nos activités humaines : sommes-nous prêts à les exercer avec plus de soin ?

Un second obstacle à la reconnaissance du soin que les éthiques du *care* nous invitent à abandonner, concerne la réduction du soin au soin médical. Une telle opération de réduction oppose ce dernier – fait d'empathie, de sollicitude, de bienveillance et de solides compétences cliniques – aux autres activités humaines, comme si celles-ci n'étaient en rien concernées par le soin. Or, le soin médical n'est qu'une des nombreuses expressions d'une visée de soin bien plus large. Par « soin », les éthiques du care entendent en effet tout ce que nous faisons pour rendre notre « monde » habitable, monde qui comprend nos corps, nos environnements sociaux, culturels et techniques, nos relations avec la nature, de telle sorte que nous puissions y vivre, nous épanouir et nous ouvrir autant que possible à toutes nos potentialités (Joan Trono, *Un monde vulnérable*). Le soin est en ce sens tout autant une visée qu'un ensemble de dispositions subjectives et de pratiques particulières dont l'œuvre est de soutenir, entretenir, protéger, permettre l'épanouissement d'un monde humain.

Comme le souligne Frédéric Worms, philosophe :

> « C'est [donc] d'abord nos vies [...] que nous [mutilerions], si nous y [réduisions] le sens de l'idée de soin, si nous en [faisions] seulement un secours urgent et en quelque sorte négatif (aussi nécessaire soit-il), sans y voir ce qu'il est toujours aussi (et qui n'est pas moins nécessaire), à savoir : une relation entre les hommes, subjective et même créatrice de subjectivité (sans laquelle nous ne serions pas des individus), une relation morale, mais aussi sociale et donc déjà politique, un rapport au monde et même un souci du monde, naturel aussi bien que culturel, écologique aussi bien que politique. » (Frédéric Worms, *Soin et politique*, Paris, Puf, 2012)

Il suit de cette conception générale du soin et de son irréductibilité au soin médical, que la santé dont une éthique du care se préoccupe ne saurait non plus être comprise à partir de sa définition strictement biomédicale. Le sens de la définition de la santé de l'OMS s'inscrit dans cet esprit : « *La santé est un état de complet bien-être physique, mental et social [qui] ne consiste pas seulement en une absence de maladie ou d'infirmité* ». La santé s'entend bien ici dans un sens plus large que la seule survie biologique des corps. Elle ne subordonne pas les destinées humaines au maintien à l'équilibre de leurs paramètres physiologiques. Vivre en santé au sens biomédical du terme, est certes un bien auquel tout un chacun tient particulièrement. Mais il s'agit aussi d'un moyen qui permet à l'homme d'accomplir son existence. Car s'il est un fait que la santé du corps contribue à celle de l'esprit, l'esprit ne se réduit pas à la vie d'un corps. Nous ne vivons pas pour la survie de notre corps, même si cette survie nous est essentielle pour vivre humainement. Cette remarque doit prémunir contre toute mécompréhension du sens d'une politique du soin. On ne peut en effet confondre une politique du soin avec une politique de santé publique qui ne se soucierait que de la survie biologique des corps, au détriment des besoins d'épanouissement sociaux, psychologiques, économiques, culturels de tout être humain en société. Si la biopolitique prend pour norme la sécurité biologique des corps, la norme d'une politique du soin doit rester le fait de vivre humainement (et pas seulement biologiquement).

Un état d'urgence sanitaire prolongé en raison d'un risque épidémique persévérant, ne peut donc pas imposer aux individus un confinement indéfini qui mettrait gravement en danger les fondements de leur épanouissement à moyen ou long terme, à moins de prévoir des aménagements nécessaires qui compenseraient ce risque. Mais si la vie en santé, au sens humain du terme, implique parfois des prises de risque (de santé au sens biologique) qui sont l'expression de la liberté et de la destinée des sujets, il n'en reste pas moins que l'art d'une politique du soin ne peut faire l'économie de la dimension collective de la santé publique, et de l'échelle populationnelle où celle-ci se situe.

Toute politique du soin digne de ce nom s'érige ainsi au cœur d'une tension, dans les compromis qu'un État doit sans cesse trouver entre les besoins individuels d'autonomie, de vie privée, de liberté d'entreprise et de mouvement de ses citoyens, et la nécessité, à des fins de santé publique, de développer des politiques incitatives (influence publique, *nudges*, etc.), instaurer des normes collectives et des mesures restrictives. Comme dans le cas de la pandémie actuelle, des comportements particuliers peuvent en effet exposer à des risques déraisonnables l'ensemble d'une population, ou certaines de ses catégories les plus vulnérables. Dans le but d'en protéger le plus grand nombre, toute politique du soin doit donc prendre acte des vulnérabilités et des interdépendances fondamentales qui lient entre eux les individus d'une population. Elle doit ensuite mesurer avec précaution les enjeux de santé publique auxquels exposent les différentes options en présence face aux risques avérés, et privilégier laquelle des orientations offre, sur une période définie, le meilleur équilibre entre la protection prioritaire – et maximale – des sujets les plus vulnérables, et un coût aussi réduit que possible en termes de limitation de mouvements, de libertés et de maux collatéraux de la pandémie, pour les individus sains ou moins exposés. C'est dans ce contexte que des technologies numériques de traçage peuvent, sous de strictes conditions développées dans ce rapport, faire partie du compromis d'une solution globale privilégiée.

Un troisième obstacle à la reconnaissance du soin que les éthiques du *care* proposent de dépasser, repose sur le préjugé que la politique et la justice n'ont rien à voir avec le soin. Concernant la politique, nos analyses précédentes mettent d'emblée en évidence la faiblesse du préjugé, qui repose sur un ensemble de réductions du soin injustifiées : une conception réaliste du soin, de ses métiers et de ses pratiques rend en effet caduque son opposition classique avec l'économie, sa relégation dans l'intimité de la sphère

domestique, ou sa réduction aux seules pratiques du soin médical. Parce que le soin est avant tout une forme de souci de soi, des autres, des institutions et de la nature, qui opère à travers un grand nombre de dispositions et de pratiques à tous les niveaux et dans toutes les dimensions de la vie en société. Il est dès lors évident que le soin ait une vocation politique, et que la politique doive s'en soucier. S'il est une œuvre politique par excellence, c'est en effet celle qui consiste, une fois reconnue son importance, à prendre soin du soin, c'est-à-dire à soutenir, par des politiques appropriées, le soutien que les hommes s'apportent, dans toutes les dimensions de leur vie. Un tel souci politique pour le soin est fondamental, car ce dernier recouvre un ensemble d'intentions et d'activités constructives, dont toute société a besoin pour donner une assise durable à ses développements sociaux, économiques, culturels, etc. L'importance politique du soin se manifeste encore dans le soin politique car le soin n'est pas seulement un soutien à l'épanouissement des vies, il est aussi la condition de leur survie. Prendre soin, c'est en effet aussi prévenir, veiller à ce que les besoins nécessaires à la vie, soient bien assurés pour que toute vie puisse s'épanouir dans une vie sociale et politique. Nous retrouvons là une condition fondamentale du contrat social et de la naissance de l'État de droit : garantir les conditions matérielles de la vie de ses citoyens.

Bref, contrairement au préjugé qui ne voit pas de soin dans la politique, ou de politique dans le soin, aucune politique à visage humain ne peut en réalité faire l'économie de la considération du soin, ni limiter le soin à l'une de ses formes particulières (médicale par exemple) sans manquer à sa tâche d'organiser et soutenir l'ensemble des moyens qui permettent aux êtres humains d'accomplir leur humanité.

Frédéric Worms y voit même là, la condition d'un renouvellement politique :

> « La politique [...] peut et doit aujourd'hui s'orienter par rapport au soin, pris dans toute sa diversité, pour, loin de s'y perdre, retrouver un sens nouveau, quelque chose comme une alternative globale. S'orienter par rapport au soin, cela ne signifie donc pas seulement repartir des secours, nécessaires et vitaux, mais s'orienter par rapport aux relations entre les individus, au *soutien*, public, à leur apporter ; le faire, de surcroît, par rapport aux relations sociales de soin, à la reconnaissance de leur réalité, de leur difficulté, des inégalités qui s'y font jour, et s'y concentrent, dans leur diversité (de la santé à l'éducation en passant par une série précise de tâches) ; ce sera s'orienter par la critique de leurs *abus* ; par l'institution des *principes* qui font que la justice participe du soin, puisque les droits et libertés mais aussi l'égalité et la solidarité, y compris dans des épreuves collectives, donc directement politiques (telles les catastrophes), sont une dimension à part entière du soin ; sans oublier, enfin, le souci pour *le monde*, qui n'implique pas seulement une politique du soin du monde, comme un objet élargi du soin, mais aussi une politique du monde (naturel et culturel) dans le soin. » (Frédéric Worms, *Soin et politique*)

L'appel, dans ces lignes, au développement d'une politique qui se soucie du soin et puisse, peut-être, y trouver comme un nouveau souffle, rejoint aussi le besoin de justice qui s'exprime dans les populations, face aux risques de nouvelles situations d'inégalités et de discriminations que la gouvernance de la crise pourrait créer, notamment en recourant à certaines technologies de traçage dans une situation d'urgence et d'impréparation démocratique. Cette demande de précaution face aux risques d'atteintes aux droits, n'est en effet pas étrangère au soin. Car contrairement au préjugé qui consiste à enclore le soin dans le registre de l'émotion ou, tout au mieux, de l'empathie et de la compassion, pour lui opposer les œuvres d'une rationalité juridique dénuée de sentiments, le souci pour la justice est une forme de soin pour les relations humaines. Nous ne dirions pas en effet d'un État injuste, délibérément générateur d'inégalités et indifférents aux discriminations, qu'il prend soin de sa population. Tout se passe plutôt comme s'il existait un lien intime entre le soin et le respect de la justice, la lutte contre les discriminations. Nous pourrions en dire autant du respect des droits et des libertés, de l'égalité et la solidarité (qui découle de l'interdépendance humaine que nous avons soulignée plus haut) : nous n'imaginons pas de pratiques de soin dignes de ce nom, cohérentes, qui ne partageraient pas ces valeurs comme constitutives de leur visée. Ainsi, de même qu'il n'y a pas de politique du soin sans soin du politique, c'est-à-dire des principes et valeurs démocratiques, il ne peut y avoir de politique du soin sans soin pour la justice, ni sans justice du soin.

Au-delà de la période particulière qui fut celle du confinement et de la mise en place des stratégies de santé publique nécessaires pour éviter l'effondrement des systèmes de santé de nombreux pays, la référence au soin dans la situation présente soulève plus que jamais la question d'une politique du soin et des conditions d'une société plus juste (un des moyens essentiels d'exercice du soin en politique étant en effet de veiller à une distribution équitable des ressources au sein du corps social).

En d'autres termes, comment prendre davantage soin de nos relations à soi, à autrui, à nos environnements, dans le monde du travail, en famille, dans les secteurs économiques et sociaux ? Comment construire les conditions d'un soin pour soi et pour autrui, pour nos relations professionnelles et privées, pour notre milieu de vie, pour la nature, qui puissent être plus en phase avec des besoins profonds rendus manifestes dans la crise traversée, et plus urgents que jamais ? La visée de soin qui suscite ce flot de questions porte avec elle un vaste espoir social : l'espoir que nous saurons tirer les conclusions de la crise que nous traversons et qu'une société plus respectueuse des droits humains émerge de la crise actuelle. Car la grande majorité des réactions dans nos sociétés occidentales en témoignent, la volonté générale de sortir de la crise, de renouer avec les activités économiques, sociales et culturelles, ne se traduit pas dans la société civile par le souhait d'un simple retour à la normale, comme s'il s'agissait de revenir en arrière, aux logiques de la globalisation d'antan, aux us et coutumes de la surveillance numérique d'autrefois, bref, au monde d'avant la crise.

Ce refus social d'un *bis repetita* de ce que nous connaissions avant la crise, doit être entendu dans nos politiques de gouvernance des technologies et de l'innovation technologique. On ne saurait envisager ainsi la mise sur le marché de technologies numériques d'aide à la sortie de crise dont la gouvernance, le design, l'implémentation et la mise en œuvre n'offriraient aucune garantie de conformité avec les principes et valeurs auxquels la société civile est plus que jamais attachée dans la situation présente. On ne pourrait également créditer le déploiement de technologies dont la gouvernance, la conception et l'évaluation ne souscriraient qu'aux principes d'une visée de soin limitée à son acception strictement biomédicale, sans considérer ses conséquences sociales, politiques, culturelles, économiques, environnementales. De la même manière, nous ne pourrions accepter une technologie dont la fonction se limiterait à sécuriser le retour des travailleurs en entreprise et la relance des activités économiques, sans considération des risques de stigmates sociaux ou des discriminations qu'elle pourrait générer. On ne saurait encore tolérer le moindre manque d'authenticité et de transparence dans la mise en œuvre de telles technologies, s'il s'avérait que leur veille sur nos comportements et nos déplacements (surveillance) n'étaient qu'en apparente conformité avec les principes et valeurs auxquels nous tenons, autrement dit si ces technologies servaient par exemple des fins particulières et cachées. Ces divers cas de figure ne répondraient pas en effet aux principes et valeurs d'un appel à « plus » de soin qui traverse tous les niveaux de la société et de nos existences. Une éthique du soin, à l'instar de l'éthique et de la déontologie médicale qui s'en inspirent,

demande de celles et ceux qui s'en réclament une transparence, une sincérité et une cohérence absolues, conditions nécessaires du respect de tout contrat social, ainsi que de la dignité et des droits de la personne humaine.

Si l'état d'urgence sanitaire déclaré face à la COVID-19 et son référentiel symbolique (imaginaire du soin) ne peuvent être confondus avec les registres de sens des états d'exception sous situation de guerre ou de lutte antiterroriste, il n'est pas moins vrai, comme nous l'avons souligné précédemment, que tout état d'exception, quelle que soit sa raison d'être, peut exposer à des risques génériques qui procèdent toujours de la possibilité de transgresser ses conditions de légitimité (non-respect de la proportionnalité des mesures engagées, absence de nécessité, traduction des ordonnances d'exception dans le droit commun...). Si la finalité d'un état d'urgence sanitaire est partagée par tous, les moyens employés peuvent parfois encore être utilisés, soit par l'État lui-même, soit par des acteurs privés, à des fins secondaires non transparentes, non démocratiquement consenties. De telles pratiques sont bien évidemment déloyales et contrastent avec l'authenticité et la sincérité d'une visée de soin partagée par le plus grand nombre dans la crise traversée. Face à ces risques toujours possibles de transgression du contrat social qu'appelle la situation présente, il est donc non seulement essentiel de bien comprendre les technologies envisagées dans la crise actuelle (Partie II du rapport), mais aussi de se doter d'une gouvernance inclusive de la sortie de crise et d'un outil d'évaluation technique, juridique et éthique approprié des technologies envisagées (Partie III du rapport). Dans la perspective d'une politique du soin en temps de crise, cet idéal de gouvernance inclusive et cet outil constituent un binôme complémentaire et nécessaire, qui devraient s'incarner avec souplesse selon les réalités du terrain, tant au niveau des entreprises, des corps intermédiaires ou de l'État que dans leurs interactions. Le but poursuivi serait de permettre à toutes les parties prenantes de la société civile de soutenir et contrôler ensemble la congruence des outils technologiques avec les principes et valeurs démocratiques auxquels tout un chacun tient face à la crise.

Notons que c'est avec ce souci à l'esprit que l'OMS, dans ses recommandations éthiques publiées le 28 mai 2020, propose les deux principes suivants pour encadrer l'utilisation des technologies de traçage numérique envisagée dans la lutte contre COVID-19, d'une façon ouverte et démocratique[18] :

UN CONTRÔLE INDÉPENDANT

Il devrait y avoir un contrôle indépendant, notamment sur les aspects éthiques et les droits de l'homme, des organismes publics et des entreprises qui développent, exploitent des applications de suivi numérique de proximité ou utilisent les informations obtenues avec ces dernières. Cette surveillance pourrait inclure la création d'un organe de contrôle indépendant. L'existence d'accords entre le gouvernement et les entreprises, ainsi que les informations nécessaires pour évaluer leur impact sur la vie privée et les droits de l'homme, doivent être rendues publiques, de même que les clauses de caducité et de contrôle. Ce dernier doit garantir que toute utilisation d'applications de suivi numérique de proximité par les gouvernements est protégée contre d'autres fonctions gouvernementales et, dans le cas des entreprises, contre d'autres intérêts commerciaux et d'affaires. Un organisme de surveillance doit également avoir accès à toutes les informations nécessaires pour s'assurer que les mesures de suivi numérique de proximité sont nécessaires et proportionnées à leur impact et à leur efficacité. Un organe de surveillance doit également contrôler la collecte et l'utilisation des données pour s'assurer qu'elles sont conformes aux lois et règlements et prévenir les abus ou l'exploitation des communautés vulnérables et marginalisées. Enfin, un organe de surveillance indépendant devrait rester en place après la fin de la pandémie pour s'assurer que toutes les technologies de suivi numérique de proximité qui ont été mises en œuvre sont entièrement démantelées. L'efficacité de tout organe de contrôle indépendant dépend en partie de l'implémentation réglementaire et de la mise en œuvre des normes éthiques, des principes et des conventions relatifs aux droits de l'homme par les gouvernements, ainsi que du respect que les gouvernements et les entreprises ont pour ces principes et ces normes.

[18] https://www.who.int/publications-detail/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

LA SOCIÉTÉ CIVILE ET L'ENGAGEMENT PUBLIC

Les réponses liées à COVID-19 qui comprennent des efforts de collecte de données devraient inclure la participation libre, active et significative des parties prenantes concernées, telles que les experts du secteur de la santé publique, les organisations de la société civile et les groupes les plus marginalisés. Cette approche participative n'est pas seulement obligatoire du point de vue de l'éthique, elle renforcera également l'adhésion, la participation volontaire et la conformité. En outre, la société civile peut jouer un rôle crucial en tenant les gouvernements et les entreprises responsables du déploiement et de l'exploitation des technologies de suivi numérique de proximité.

Au regard de ces éléments, des technologies numériques de soutien à la sortie de crise ne pourraient être implémentées qu'à la condition que leur conception, leur implémentation et leur usage fassent l'objet d'une évaluation rigoureuse au nom de la société civile et par ses représentants, qui garantissent leur conformité aux termes du contrat social qu'appelle la situation présente. Dans le plein respect de ces conditions, et à condition bien sûr que leur efficacité soit vérifiée, nous ne devrions pas nous inquiéter que de telles technologies soient parfois privilégiées dans certaines situations porteuses de dilemmes éthiques, lorsque l'analyse des valeurs en présence démontre aux yeux de toutes et tous, que la solution technologique pourrait permettre de favoriser la moins mauvaise des issues au regard d'une visée du soin communément partagée.[19]

Ces remarques rejoignent profondément les conditions d'une politique du soin cohérente, qui se doit toujours d'être éminemment inclusive et participative, en raison de la nature même de son objet (le soin). En effet, s'il n'y a pas de politique qui n'émerge d'un souci (*care*) pour le gouvernement des hommes comme un ordre qui le redouble, un soutien institutionnellement organisé aux soutiens que les hommes se prêtent les uns aux autres, le soin est toujours éminemment empirique et situé. Toute visée de soin s'observe en effet dans les pratiques sociales de celles et ceux qui la mettent en œuvre dans leurs environnements de travail et d'engagement. En effet, tout souci de soi, des autres et du monde, présuppose toujours l'exercice d'un ensemble de compétences toujours particulières, souvent apprises d'expérience et adaptées aux enjeux de situations précises (parentales, sociales, éducatives, environnementales, culturelles, économiques, politiques…). Ces pratiques s'inscrivent elles-mêmes dans des institutions très diverses, dans des procédures d'évaluation, dans des contrats d'objectifs, dans des politiques locales et des cultures concrètes. La science du soin n'est en ce sens jamais « fondamentale » ou « généraliste ». Elle est toujours de nature éminemment pragmatique, « contexte-dépendante » et particulière.

En conséquence, une politique du soin au niveau de l'État, des corps intermédiaires (fédérations, corporations,…), des entreprises, ou entre ces instances, ne peut se passer des perspectives, des idées, du feed-back et des compétences des acteurs des différents terrains où s'opérationnalise le soin. Elle ne peut ignorer leurs attentes, leurs besoins et leurs évaluations. Elle doit se penser, se construire et s'ajuster chemin faisant en dialogue avec toute les parties engagées dans les formes du soin auxquelles elle souhaite apporter son soutien. Une politique du soin cohérente demande donc « par essence » (étant donné la nature de son intention et de son objet) que des processus institutionnels soient imaginés et mis en œuvre aux différents niveaux de la société civile pour garantir la consultation et permettre la participation de toutes les parties prenantes à l'élaboration des politiques du soin et à leur évaluation continue, en dialogue serré avec les expériences des terrains où s'exerce le souci de soi, des autres et du monde. Éminemment participative, toute politique du soin doit être aussi inclusive, en se souciant de la participation de tous les prestataires et les bénéficiaires – y compris les plus vulnérables, ou les moins visibles – des pratiques de soin qui assurent les conditions de base d'un épanouissement humain souhaité accessible pour toutes et tous dans une société de droits.

[19] Les arguments d'une telle position sont discutés dans un bel article rédigé par Michaël Parker, Christophe Fraser et leurs collègues : **https://jme.bmj.com/content/early/2020/05/05/medethics-2020-106314**

REMARQUE : Le présent gabarit d'étude d'impact PostCoviData a été élaboré par les membres d'ITechLaw dont les noms figurent à l'annexe 3, dans le cadre du projet PostCoviData ayant été réalisé sous la direction de la Human Technology Foundation. C'est à titre personnel que les contributeurs de ce gabarit ont participé à son élaboration. C'est pourquoi les opinions exprimées dans celui-ci ne reflètent le point de vue d'aucun cabinet juridique ou d'autres entités pouvant leur être affiliées.

Le présent gabarit est communiqué à des fins d'information seulement. Il ne constitue pas un conseil juridique. Il est diffusé à titre d'exemple des principaux types de renseignements susceptibles d'être pris en compte dans le cadre du processus d'étude d'impact PostCoviData (« EIP ») à appliquer à la solution Pandemic Tech. En consultation avec un conseiller juridique compétent, vous devez l'adapter lorsqu'il y a lieu, de sorte qu'il puisse répondre à vos besoins.

ANNEXE 2

LE POSTCOVIDATA IMPACT ASSESSMENT

[Responsable du projet]
[Titre du projet]
Étude d'impact PostCoviData (« EIP »)

<Jour> <Mois> <Année>

1. RÉSUMÉ DU PROJET

(Décrire la solution Pandemic Tech, les ensembles de données utilisées et le contexte)

Dans le présent document, la « **solution Pandemic Tech** » désigne une solution logicielle, un dispositif ou encore un produit qui est développé ou déployé par l'entité responsable du projet et qui intègre des fonctionnalités reposant sur des données.

Décrire le projet et ses objectifs, en traitant des points clés suivants :

- *Description de la solution Pandemic Tech dans sa globalité, y compris la présentation d'une description / d'un aperçu fonctionnel et des ensembles de données utilisés.*
- *À quoi sert la solution Pandemic Tech ?*
- *Dans quel contexte sociopolitique le déploiement ou l'utilisation de la solution Pandemic Tech s'inscrit-il ?*
- *La solution Pandemic Tech soulève-t-elle des enjeux relativement à des préoccupations particulières en matière d'éthique qui doivent être examinés préalablement à sa mise en œuvre ?*
- *À quelle étape du projet l'EIP doit-elle être effectuée ? Le calendrier du projet est-il appelé à changer ?*
- *À quels objectifs de l'entité responsable du projet la solution Pandemic Tech doit-elle permettre de répondre ?*
- *La solution Pandemic Tech se rattache-t-elle à une initiative ponctuelle ou fait-elle partie d'une stratégie de développement commercial continu ?*

Résumé du projet

[REMARQUE : La solution Pandemic Tech s'inscrit-elle dans le prolongement d'une activité antérieure ? *Dans l'affirmative, déterminer si elle a déjà fait l'objet d'une évaluation. Si une évaluation a déjà été effectuée, dans quelle mesure et pourquoi les activités relatives aux données s'y rattachant ont-elles changé (se reporter à l'évaluation précédente) ?]*

Diagramme de flux de données

Structure de gouvernance

2. PRINCIPAUX FACTEURS À PRENDRE EN COMPTE DANS LA RÉALISATION D'UNE EIP

La première étape d'une étude d'impact complémentaire visant une solution Pandemic Tech doit consister à évaluer les raisons pour lesquelles celle-ci requiert une telle EIP, compte tenu de toute évaluation de l'incidence sur les risques déjà effectuée.

Pour exécuter cette première étape, l'entité responsable du projet doit définir clairement le champ d'application, les objectifs et les caractéristiques de la solution Pandemic Tech. À cette étape, de nombreux éléments doivent être pris en compte, mais il n'est pas nécessaire que l'analyse à effectuer soit aussi approfondie que celle qui doit être réalisée dans le cadre de l'évaluation principale. Les critères importants à considérer sont énumérés dans le tableau ci-dessous. (Veuillez prendre note qu'il s'agit d'une liste non exhaustive qui doit être adaptée selon le contexte particulier de l'entité responsable du projet). Il est à noter que cette EIP devra être continuellement adaptée à mesure que la communauté scientifique confirmera les caractéristiques de la pandémie. Elle devra également être adaptée en fonction de l'évolution des connaissances sur les effets des solutions technologiques sur les gens et les sociétés.

Aussi bien à cette étape préliminaire que dans le cadre de l'évaluation des principaux risques, l'évaluation des facteurs de risque doit reposer sur une échelle d'évaluation des risques allant de « faible » à « élevé » (Faible, Modéré, Élevé). Il est recommandé d'appliquer une approche globale et contextuelle. Au cours de l'application d'une telle approche, les facteurs de risque identifiés devront être évalués en fonction de leur interaction les uns avec les autres. Par exemple, on peut considérer que le déploiement strictement interne d'une solution Pandemic Tech sur laquelle reposent certains processus décisionnels présente généralement moins de risques qu'un système axé sur la prestation de services aux citoyens. Néanmoins, l'utilisation interne d'une solution Pandemic Tech axée sur l'évaluation ou la surveillance des employés peut déclencher l'obligation de se conformer à certaines dispositions en matière de droit du travail, de sorte qu'une telle solution peut présenter davantage de risques que certains systèmes axés sur la prestation de services aux citoyens.

Facteurs justifiant de procéder à une étude d'impact	Cote de risque (Faible, Modéré, Élevé)	Commentaire
1. Dans quel contexte la solution Pandemic Tech sera-t-elle utilisée ou déployée ? S'agit-il d'un contexte de prestation de services aux citoyens ?		
2. Cette solution est-elle destinée à être utilisée dans un pays où la protection des données est assurée en vertu de dispositions législatives ou réglementaires ? S'agit-il d'un pays où prévaut l'État de droit ? La solution Pandemic Tech est-elle destinée à être déployée dans un cadre juridique exceptionnel (état d'urgence) ?		
3. La solution Pandemic Tech est-elle destinée à être utilisée à l'échelle de divers territoires ayant un cadre juridique propre (à l'échelle de divers États, provinces ou pays) ?		
4. Quelles catégories de personnes contribueront à la solution Pandemic Tech ?		
5. Quels sont le type et l'origine des données qui seront utilisées dans le cadre de la formation sur la solution Pandemic Tech ? Dans le contexte d'utilisation d'une solution reposant sur l'IA, des données à caractère personnel feront-elles partie des données de formation ? Quel est le niveau de sensibilité des données à caractère personnel ? Sur qui ces données portent-elles ?		
6. Quel type de décisions la solution Pandemic Tech permettra-t-elle de prendre ? Quels seront les droits et intérêts en jeu ? S'agit-il de droits fondamentaux ou de droits de la personne ?		
7. Quel est le degré d'autonomie attendu de la solution Pandemic Tech ? Par exemple, des opérateurs ou des décideurs humains superviseront-ils la prise des décisions fondées sur l'intelligence artificielle (IA), le cas échéant ? À quelle fréquence cette supervision sera-t-elle effectuée ? Quelles dispositions seront adoptées pour éviter le biais de l'automatisation ou de l'ancrage de la solution Pandemic Tech ?		
8. Quelles caractéristiques de la solution Pandemic Tech pourraient influer sur la capacité d'expliquer et de vérifier les algorithmes sur lesquels elle repose ? Est-il possible de décrire la solution Pandemic Tech ?		
9. Quel sera le degré de contrôle ou de responsabilité de l'entité responsable du projet à l'égard de la version définitive de la solution Pandemic Tech ? Quels tiers sont censés y contribuer ?		
Synthèse (la question de savoir si la présente EIP complémentaire est requise/utile ou non et la présentation des principaux points permettant d'en arriver à cette conclusion) :		

3. ÉVALUATION PRINCIPALE

À chacune des rangées du tableau ci-dessous figure une synthèse des principales exigences se rattachant aux principes de responsabilité associés à la solution Pandemic Tech ainsi qu'un aperçu des principales questions ou considérations que vous devez aborder. Pour savoir quels sont les documents à consulter et quels sont les renseignements à consigner dans ce tableau, veuillez vous reporter aux listes de contrôle figurant à l'annexe 1.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
Principe 1 : But éthique et avantage pour la société *Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech et toute législation nationale réglementant une telle utilisation doivent exiger que les objectifs de cette mise en œuvre soient identifiés et veiller à ce que ces objectifs soient compatibles avec les objectifs éthiques généraux de bienfaisance et de non-malfaisance, ainsi qu'avec les autres principes applicables.*				
Aperçu du principe · L'entité responsable du projet doit passer en revue les objectifs associés à la solution Pandemic Tech (p. ex., assurer une prise de décisions cohérentes, l'amélioration de l'efficacité opérationnelle et la réduction des coûts ou la mise en marché de nouvelles caractéristiques de produits axée sur la diversification des choix offerts aux citoyens). Elle doit ensuite pondérer ces objectifs en fonction des risques liés à l'utilisation de la solution Pandemic Tech dans le cadre de son processus décisionnel. · L'entité responsable du projet doit réunir les principales parties prenantes requises à des fins de discussions / de prise de décisions, dont les suivantes : – Les parties prenantes internes (gestionnaires de projet, scientifique en chef, dirigeants, administrateurs, employés, membres de la société civile, etc.) – Les parties prenantes externes (développeurs, fournisseurs de données externes, partenaires de recherche, distributeurs, etc.) – Les utilisateurs finaux (citoyens, utilisateurs de services, etc.) – Les autorités publiques (institutions publiques, organismes de réglementation, etc.) – Les membres de groupes vulnérables nécessitant des soins particuliers (enfants, personnes handicapées, personnes dont la culture technologique est limitée, etc.) En déterminant le degré de supervision humaine requise, l'entité responsable doit prendre en compte l'incidence des décisions prises à l'aide de la solution Pandemic Tech sur le plan individuel, sur des groupes de personnes et sur la société en général. C'est sur cette base qu'elle doit déterminer le niveau d'intervention humaine requis dans le processus décisionnel reposant sur la solution Pandemic Tech.				
PARTIE I – ÉVALUATION GÉNÉRALE APPLICABLE À TOUTES LES SOLUTIONS TECHNOLOGIQUES				
1. Quelles sont les dispositions législatives régissant la collecte, l'analyse et l'utilisation des données ?				
2. Y a-t-il d'autres obligations légales, transfrontalières, politiques, contractuelles, sectorielles ou autres en lien avec la collecte, l'analyse ou l'utilisation des données ?				
3. Est-il possible que la solution Pandemic Tech soit assimilable à un dispositif médical ou à toute autre caractéristique faisant en sorte qu'elle soit assujettie à des dispositions réglementaires particulières (p. ex., le secret médical) susceptibles d'en modifier la perception d'un point de vue éthique ?				
4. La solution Pandemic Tech est-elle conforme aux valeurs, aux normes et aux politiques de l'entité responsable du projet ?				
5. Quels sont les risques d'atteinte à la réputation et les risques significatifs potentiels de l'entité responsable du projet ?				
6. Le déploiement ou l'utilisation de la solution Pandemic Tech aura-t-il une incidence sur l'autonomie des parties prenantes concernées ?				
7. Prendre en compte les sauvegardes appropriées permettant de promouvoir de façon éclairée la capacité d'agir, l'autonomie et la dignité des employés, ainsi que d'éviter les effets inappropriés ou destructeurs sur leur santé émotionnelle ou psychologique (monotonie des tâches, surveillance excessive, fausser le comportement, exposition soutenue à du contenu horrifiant).				
8. Prendre en compte toutes les autres sauvegardes appropriées à évaluer, telles que la suppression automatique de données à l'expiration d'un délai donné.				

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
PARTIE II – ÉVALUATION PROPRE AUX SOLUTIONS REPOSANT SUR L'IA ET L'APPRENTISSAGE AUTOMATIQUE				
9. Se demander si, d'un point de vue technologique, il est possible de faire en sorte que toutes les occurrences possibles soient programmées à l'avance dans la solution Pandemic Tech, de façon à en assurer la cohérence comportementale. Si ce n'est pas le cas, se demander comment les résultats (aussi appelés « comportements machines ») seront contrôlés, puis réintégrés dans le cadre de gouvernance et de supervision.				
Synthèse du principe · *La solution Pandemic Tech est-elle compatible avec la capacité d'agir et l'autonomie humaines ainsi qu'avec le respect des droits fondamentaux de la personne ?* · *La solution Pandemic Tech est-elle conforme aux objectifs éthiques généraux de bienfaisance et de non-malfaisance ?* · *Quels sont les risques de préjudice pour les personnes et leurs droits en lien avec la solution Pandemic Tech ?* – Devrait notamment être considérée comme étant un facteur de risque la possibilité accordée aux gens de refuser l'installation de la solution et de la désinstaller ou de l'enlever de leurs dispositifs. – Devrait également être prise en compte la proportionnalité de la collecte de données dans les dispositifs par rapport aux objectifs associés à la solution. – Devrait aussi être prise en compte la question de savoir si l'entité responsable du projet a mis en œuvre des mesures efficaces faisant en sorte que le contrôle et la supervision du processus décisionnel automatisé reposant sur la solution, s'il y a lieu, soient assurés par des humains. – Devrait également faire l'objet d'une investigation l'incidence globale potentielle de l'utilisation de la solution sur les parties prenantes autres que l'utilisateur final.				
Principe 2 : Responsabilité Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech et toute législation nationale réglementant une telle utilisation doivent respecter et adopter les sept principes de l'énoncé de politique pour une IA responsable (ou d'autres principes de responsabilité analogues). Dans tous les cas, les humains doivent rester responsables des actes et des omissions des systèmes reposant sur des données. **Aperçu du principe** — L'entité responsable du projet doit s'assurer en tout temps de rester redevable à l'égard du déploiement éthique et responsable des solutions Pandemic Tech dont elle s'occupe, notamment lorsqu'il s'agit d'un déploiement « avec intervention humaine ».				
PARTIE I – ÉVALUATION GÉNÉRALE APPLICABLE À TOUTES LES SOLUTIONS TECHNOLOGIQUES				
1. La solution Pandemic Tech est-elle centralisée ou décentralisée ?				
2. Quel est le niveau d'appui interne, notamment sur le plan financier, à la solution Pandemic Tech ?				
3. Au sein de l'entité responsable du projet, de qui relèvera la solution Pandemic Tech ? Cette entité dispose-t-elle d'une instance de coordination centrale ? Qui, au sein de l'entité responsable du projet, devra rendre des comptes en cas de défaillance de la solution Pandemic Tech ou en cas de production de résultats défavorables pour ses utilisateurs ?				
4. Quels rôles l'entité responsable du projet assume-t-elle dans le cadre du processus de mise en œuvre de la solution Pandemic Tech (utilisateur final, développeur, fournisseur de données, etc.) ?				
5. Un commissaire indépendant (p. ex., une agence gouvernementale ou un fonctionnaire désigné) est-il chargé d'examiner et de contrôler des solutions telles que la solution Pandemic Tech ?				
6. Les membres du personnel recevront-ils de la formation sur l'utilisation de la solution Pandemic Tech ? Les membres du personnel et les services concernés sont-ils parfaitement au fait de leurs rôles et responsabilités ? Cette enquête doit prendre en compte les différentes catégories de personnel et les différents échelons appelés à participer à la conception de la solution Pandemic Tech (p. ex., gestion/supervision et niveaux de programmation).				

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
7. Dans quelle mesure l'utilisation interne de la solution Pandemic Tech par l'entité responsable du projet aura-t-elle une incidence sur les rôles et les tâches des employés ?				
8. Quelles composantes du « processus d'approvisionnement » des services de formation et de perfectionnement ont été externalisées ? Si la prestation de tels services a été confiée à un tiers, celui-ci est-il soumis à un contrôle qualité du même niveau que celui qu'applique l'entité responsable du projet ?				
9. Dans quelle mesure la solution Pandemic Tech est-elle tributaire de l'apport de données ou de systèmes tiers ? Dans quelle mesure les obligations de reddition de comptes s'appliquent-elles aux tiers appelés à intervenir ?				
10. Des méthodes de contrôle qualité externes ont-elles été observées dans le cadre de la création de la solution Pandemic Tech (p. ex., la norme ISO 9001) ?				
PARTIE II – ÉVALUATION PROPRE AUX SOLUTIONS REPOSANT SUR L'IA ET L'APPRENTISSAGE AUTOMATIQUE				
11. S'il y a lieu, comment le processus de sélection d'un modèle d'IA et de formation sur ce modèle sera-t-il géré ?				
12. S'il y a lieu, prendre en compte les activités de maintenance, de surveillance, de documentation et d'examen des modèles d'IA déployés.				
13. S'il y a lieu, prendre en compte les divers degrés de supervision humaine dans le cadre du processus décisionnel : a) **Modèle avec intervention humaine :** Ce modèle suppose la supervision et la participation actives d'opérateurs humains dans le processus décisionnel, ceux-ci en conservant pleinement le contrôle, tandis que l'IA génère seulement des recommandations ou des suggestions. Aucune décision ne peut être prise sans qu'un humain ne la corrobore, p. ex., en activant la commande permettant d'exécuter une décision donnée. (N.B. Prendre également en compte la notion d'« **intervention humaine** » lorsqu'un biais de l'automatisation, de l'ancrage ou de la confirmation est constaté chez un opérateur humain. Le rôle de celui-ci consiste essentiellement à accepter le résultat généré par l'IA, sans l'évaluer de façon critique pour déterminer s'il est exact ou non). b) **Modèle sans intervention humaine :** Ce modèle suppose que l'exécution des décisions prises ne fait l'objet d'aucune supervision humaine. La prise de décisions est entièrement sous le contrôle de l'IA, sans possibilité pour un opérateur humain de rejeter les décisions prises par celle-ci. c) **Modèle avec supra-intervention humaine :** Ce modèle permet aux opérateurs humains d'ajuster les paramètres au cours de l'exécution des algorithmes.				
14. La solution Pandemic Tech suppose-t-elle le développement, le déploiement ou l'utilisation d'une solution reposant sur l'IA ou d'une combinaison des trois types de modèles ?				
15. Quels sont les droits et intérêts en jeu dans le cadre de la prise de décisions automatisée par la solution Pandemic Tech ?				

Synthèse des principes

- Le cadre de gouvernance de la solution Pandemic Tech doit notamment être pris en compte, en vérifiant qu'il permet d'assurer le respect des droits et intérêts des utilisateurs.
- Les sauvegardes mises en œuvre pour assurer l'indépendance de la solution Pandemic Tech doivent également être prises en compte.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
Principe 3 : Transparence et explicabilité *Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech et toute législation nationale réglementant une telle utilisation doivent s'assurer que, dans la mesure du raisonnable compte tenu des circonstances et de la technologie de pointe, cette utilisation est transparente et que les résultats des décisions prises à l'aide d'un tel système reposant sur les données sont explicables.* **Aperçu du principe** · L'entité responsable du projet doit assurer en tout temps la transparence de la solution Pandemic Tech, notamment en informant les parties prenantes concernées : a) du fait que la solution Pandemic Tech est en cours d'utilisation ; b) des fins visées par la solution Pandemic Tech ; et c) de l'identité de la personne pouvant répondre à leurs questions concernant la solution Pandemic Tech. Il est possible de renforcer la transparence en s'appuyant sur les notions d'explicabilité, de répétabilité et de traçabilité. · L'intensité des obligations en matière de transparence et d'explicabilité varie en fonction de divers facteurs, dont la nature des données visées, le résultat des décisions ayant été prises et les conséquences qui en découlent pour la personne concernée. Les entités responsables de projets qui développent la solution Pandemic Tech doivent s'assurer que l'architecture système, la logique algorithmique, les ensembles de données, les méthodes de test et l'ensemble des politiques et procédures relatives aux activités de développement et aux activités opérationnelles connexes utilisées servent à l'intégration de la transparence et de l'explicabilité dans le cadre de la conception.				
PARTIE I – ÉVALUATION GÉNÉRALE APPLICABLE À TOUTES LES SOLUTIONS TECHNOLOGIQUES				
1. Des modalités d'utilisation claires et faciles à lire sont-elles transmises aux utilisateurs de la solution Pandemic Tech ?				
2. Ces modalités d'utilisation prévoient-elles des procédures de partage de données ? Y a-t-il des problèmes d'incohérence entre ce qui est indiqué dans les modalités d'utilisation et les modalités de fonctionnement reconnues de la solution Pandemic Tech ?				
3. L'entité responsable du projet dispose-t-elle d'une politique de protection des données à caractère personnel ?				
4. L'entité responsable du projet communique-t-elle de l'information sur l'ampleur de l'adoption de la solution Pandemic Tech ? De l'information de cet ordre est-elle accessible à l'extérieur de cette entité ?				
5. L'entité responsable du projet fait-elle preuve de transparence à l'égard des résultats générés par la solution Pandemic Tech (p. ex., taux de faux positifs et de faux négatifs associés à une application de traçage des contacts) ?				
6. L'entité responsable du projet sait-elle quelles sont les données utilisées par la solution Pandemic Tech et la façon dont elles sont utilisées dans le cadre du processus décisionnel ? Serait-elle en mesure d'expliquer la solution Pandemic Tech au public ?				
7. Les données d'origine comprennent-elles des informations exclusives ?				
8. Les données d'origine comprennent-elles des données anonymisées ou synthétisées ? Les résultats générés par la solution Pandemic Tech auraient-ils été plus exacts, plus bénéfiques ou moins à risque de biais s'ils avaient compris des données à caractère personnel ?				
9. Les données d'origine comprennent-elles des données à caractère personnel ?				
10. La solution Pandemic Tech est-elle vérifiable ? La vérifiabilité renvoie au degré de préparation d'une solution Pandemic Tech en vue d'une évaluation des algorithmes, des données et des processus de conception sur lesquels elle repose.				
11. La solution Pandemic Tech est-elle une solution robuste ? La robustesse renvoie à la capacité d'un système informatique de composer avec des erreurs dans le cadre de l'exécution, ainsi qu'avec des données d'entrée erronées. Elle est évaluée en fonction de la mesure dans laquelle un système ou une composante peut fonctionner correctement en la présence de données d'entrée invalides ou de conditions environnementales difficiles.				

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
12. L'entité responsable du projet est-elle en mesure de procéder à une évaluation de la solution, ou y est-elle préparée, de façon à permettre la détection de la cause de tout résultat discriminatoire ou défavorable généré par la solution Pandemic Tech ?				
PARTIE II – ÉVALUATION PROPRE AUX SOLUTIONS REPOSANT SUR L'IA ET L'APPRENTISSAGE AUTOMATIQUE				
13. Quel est le degré général d'opacité de la solution Pandemic Tech (c.-à-d. la mesure dans laquelle celle-ci peut être décrite comme une « boîte noire ») ?				
14. Quel est le type de modèle d'IA employé pour créer la solution Pandemic Tech, le cas échéant ?				
15. Est-il possible pour un spécialiste de comprendre la façon dont la solution Pandemic Tech prend ses décisions et aboutit à une conclusion précise dans un cas précis ?				
16. Envisager de concevoir la solution Pandemic Tech graduellement en commençant par le niveau le plus fondamental afin de favoriser la transparence et l'explicabilité dès la conception.				
17. Quels sont les risques liés à des décisions inexplicables fondées sur l'IA pour les droits et les intérêts des parties prenantes, le cas échéant ?				
18. Quelles sont les attentes des différentes parties prenantes en matière de transparence et d'explicabilité ?				
19. Quel est le degré d'expertise des personnes qui recevront l'explication (spécialiste en IA, profane, profane instruit, etc.) ?				
20. Dans quelle mesure cette donnée serait-elle utile pour les personnes à l'extérieur de l'entité responsable du projet afin de comprendre le système d'IA et ses décisions ? Les utilisateurs finaux seraient-ils encouragés à déjouer la solution Pandemic Tech ou capables de le faire, s'ils en connaissaient le processus décisionnel ?				
21. La solution Pandemic Tech est-elle explicable ? L'entité responsable du projet devrait être en mesure d'expliquer à un tiers la façon dont fonctionnent les algorithmes de la solution et la façon dont le processus décisionnel intègre la prédiction d'un modèle.				
22. La solution Pandemic Tech est-elle répétable ? La répétabilité s'entend de la possibilité d'exécuter une action ou de prendre une décision de façon constante dans un scénario donné. La constance d'exécution pourrait fournir un certain degré de confiance aux utilisateurs de l'IA.				
23. La solution Pandemic Tech est-elle reproductible ? La reproductibilité désigne la possibilité pour une équipe de vérification indépendante de produire des résultats identiques en utilisant la même méthode d'IA que celle décrite dans la documentation préparée par l'entité responsable du projet.				
24. La solution Pandemic Tech est-elle traçable ? Une solution est considérée comme étant traçable si ses processus décisionnels sont documentés d'une manière facile à comprendre.				

Synthèse du principe

- La documentation mise à la disposition des utilisateurs et le degré de clarté de celle-ci doivent notamment être évalués.
- Tout problème d'opacité touchant une partie ou la totalité de la solution Pandemic Tech doit notamment être mis en évidence.
- Les choix effectués par l'entité responsable du projet à l'égard des ensembles de données utilisés aux fins de la solution Pandemic Tech doivent également être synthétisés.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
Principe 4 : Équité et non-discrimination *Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech et toute législation nationale ou norme de référence internationale réglementant une telle utilisation doivent garantir la non-discrimination des résultats fondés sur des données et promouvoir des mesures efficaces et appropriées pour garantir une utilisation équitable.* **Aperçu du principe** · L'utilisation de la solution Pandemic Tech doit être non discriminatoire sur le plan de l'accessibilité. Cette solution devrait être accessible également aux personnes ayant un handicap (par exemple, une capacité visuelle limitée). · Les décisions fondées sur la solution Pandemic Tech doivent être équitables et non discriminatoires d'après les mêmes normes que celles visant les processus décisionnels relevant entièrement de l'humain. Le développement de l'IA doit être conçu de manière à privilégier l'équité. · Cela signifie d'aborder les algorithmes et les biais de données dès le début afin de garantir l'équité et la non-discrimination.				
PARTIE I – ÉVALUATION GÉNÉRALE APPLICABLE À TOUTES LES SOLUTIONS TECHNOLOGIQUES				
1. Les données sont-elles de grande qualité ? Les facteurs suivants doivent être pris en considération : – l'exactitude de l'ensemble de données, s'agissant de la mesure dans laquelle les valeurs incluses dans l'ensemble de données reflètent adéquatement les véritables caractéristiques des entités décrites par l'ensemble de données ; – l'exhaustivité de l'ensemble de données, tant sur le plan des attributs que sur celui des éléments de l'ensemble ; – la véracité de l'ensemble de données, soit la crédibilité des données, y compris la question de savoir si elles proviennent d'une source fiable ; – le temps écoulé depuis la compilation ou la mise à jour de l'ensemble de données ; – la pertinence de l'ensemble de données et le contexte dans lequel les données ont été recueillies, sachant que ces facteurs peuvent influer sur l'interprétation des données et la mesure dans laquelle on s'appuiera sur les données aux fins prévues ; – l'intégrité de l'ensemble de données obtenu à partir de plusieurs ensembles de données, nommément la qualité de la transformation et de l'extraction ; – la convivialité de l'ensemble de données, notamment la mesure dans laquelle il est structuré d'une manière compréhensible pour une machine ; – le caractère utilisable de toute donnée à caractère personnel contenue dans les ensembles de données, notamment en ce qui a trait à l'obtention des consentements requis ; et – les interventions humaines, p. ex. si l'humain a filtré les données, leur a attribué des étiquettes ou les a éditées.				
2. Envisager de réduire au minimum les biais inhérents : – Biais de sélection : Survient lorsque les données utilisées pour produire la solution Pandemic Tech ne sont pas entièrement représentatives des données réelles que peut recevoir la solution Pandemic Tech ou de l'environnement réel dans lequel la solution peut fonctionner. Le biais d'omission et le biais de stéréotype sont des exemples courants de biais de sélection dans un ensemble de données. – Biais de mesure : Survient lorsque le dispositif de collecte de données fait en sorte que les données sont systématiquement biaisées dans un sens en particulier. – Les facteurs suivants doivent être pris en considération : · la fréquence à laquelle l'ensemble de données est revu et mis à jour ; · la diversité de l'ensemble de données, et la variété des sources d'où proviennent les données (données numériques, texte, audio, visuelles, transactionnelles, etc.) ; et · le caractère utilisable de différents ensembles de données, notamment la façon dont ils ont été appariés et nettoyés afin que des ensembles de données relationnels puissent être corrélés et reliés.				

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
3. La solution Pandemic Tech prend-elle des décisions automatisées ayant une incidence sur les droits et les intérêts de gens ou d'entreprises ? – Déterminer notamment si la solution Pandemic Tech peut avoir comme conséquence pour l'utilisateur de faire l'objet d'un traitement différencié qui serait autrement interdit en vertu de la législation applicable.				
4. L'utilisation de la solution Pandemic Tech est-elle volontaire, encouragée ou obligatoire ?				
5. La solution Pandemic Tech fait-elle l'objet de tests rigoureux, aussi bien avant son utilisation que de façon périodique par la suite, afin d'éviter tout effet préjudiciable pour une catégorie de personnes protégées ?				
6. Est-il possible que certaines catégories de personnes se sentent exclues du bassin des utilisateurs de la solution Pandemic Tech ? – Les caractéristiques de conception prennent-elles en compte les besoins des personnes âgées ? (Par exemple, s'agit-il d'une solution conviviale ?) – Les caractéristiques de conception prennent-elles en compte les besoins des personnes ayant un handicap ? À consulter : L'initiative sur l'accessibilité du Web réalisée par le World Wide Web Consortium				
7. L'entité responsable du projet est-elle dotée d'un système lui permettant d'intervenir lorsque la solution Pandemic Tech produit des résultats discriminatoires ou inéquitables, et de résoudre pareille situation ? – Prendre en compte la capacité de l'entité responsable du projet à évaluer et à repérer des ensembles de données biaisés, les éventuelles mesures d'atténuation fournies aux utilisateurs finaux et toute possibilité de reconcevoir la solution Pandemic Tech.				
PARTIE II – ÉVALUATION PROPRE AUX SOLUTIONS REPOSANT SUR L'IA ET L'APPRENTISSAGE AUTOMATIQUE				
8. Quelles méthodologies ont été appliquées dans le cadre de l'apprentissage de la solution Pandemic Tech ?				
9. La solution Pandemic Tech comporte-t-elle une phase d'apprentissage déterminée suivie d'une phase d'utilisation statique, ou s'améliore-t-elle en continu ? Si tel est le cas, comment les améliorations sont-elles filtrées pour détecter tout biais et évaluer la qualité, notamment ?				
10. Quels sont les risques de biais liés à 1) l'algorithme, 2) les données de formation, 3) les développeurs et 4) les utilisateurs finaux ?				
11. Quels sont les risques d'atteinte à la réputation que courent les entités responsables de projets dans l'éventualité où la solution Pandemic Tech prendrait des décisions automatisées biaisées ?				
12. Comment la solution Pandemic Tech gère-t-elle les « cas limites » ?				
13. Les données de formation utilisées pour la solution Pandemic Tech sont-elles représentatives de la population à l'égard de laquelle la solution prendra des décisions (exactitude, qualité et exhaustivité des données) ?				
14. L'entité responsable du projet a-t-elle mis en place un processus de sélection rigoureux relativement aux ensembles de données de formation de la solution Pandemic Tech ? Par exemple, y a-t-il des critères minimaux à respecter quant à la diversité et à la qualité des ensembles de données utilisés ?				

[1] Précité, note 11.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
15. La solution Pandemic Tech utilise-t-elle des ensembles de données différents pour l'apprentissage, les tests et la validation ? Biais de pondération : Survient lorsque des pondérations différentes sont attribuées aux données utilisées par la solution d'IA pour la production du résultat pertinent. Des ensembles de données peuvent être associés à une valeur plus ou moins grande de façon arbitraire ou inexacte.				
Synthèse du principe · Synthétiser les biais inhérents à la solution Pandemic Tech, le cas échéant. · Tout problème de discrimination ou de restriction potentielle quant à l'utilisation de la solution Pandemic Tech par certaines catégories de personnes doit notamment faire l'objet d'une évaluation. · Il importe notamment de répondre au risque de toute utilisation inappropriée de la solution Pandemic Tech.				
Principe 5 : Sécurité et fiabilité *Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech et toute législation nationale réglementant une telle utilisation doivent adopter des régimes et des normes de conception garantissant une sécurité et une fiabilité élevées des systèmes fondés sur des données tout en limitant l'exposition des développeurs et des entités procédant aux déploiements de tels systèmes.* **Aperçu du principe** L'entité responsable du projet doit tester la solution Pandemic Tech de manière rigoureuse afin de s'assurer qu'elle adhère de manière fiable aux principes éthiques et moraux sous-jacents et que son apprentissage repose sur des données soigneusement conservées et aussi « exemptes d'erreur » que possible, dans les circonstances				
PARTIE I – ÉVALUATION GÉNÉRALE APPLICABLE À TOUTES LES SOLUTIONS TECHNOLOGIQUES				
1. Si l'entité responsable du projet ne détient pas de certifications de sécurité de l'information reconnues à l'échelle internationale (p. ex., ISO/IEC 2700), quel est le niveau actuel des mesures de sécurité ayant été adoptées ? Prendre en compte notamment les mesures ci-après : détection des incidents de sécurité, intervention et gestion, plans de continuité des activités, politiques de gestion du changement.				
2. Quel est l'historique de l'entité responsable du projet à l'égard de violations de données et d'incidents liés aux données ? Comment cette entité est-elle intervenue pour faire face aux violations de données et aux incidents liés aux données passés ?				
3. Quels sont les risques liés à la cybersécurité et les vulnérabilités de la solution Pandemic Tech ? Qui est exposé à un risque de préjudice ? Quelles sont les mesures préventives en place ?				
4. Relativement aux gens qui accèdent aux données, la confidentialité est-elle assurée ?				
5. Quelles sont les possibilités de subversion de l'utilisation prévue (dans le cas de technologies pouvant servir à un « double usage ») ?				
6. Quelles sont les attentes des clients en matière de sécurité et de fiabilité, et quel est leur degré d'expertise ?[1]				
7. Quelles sont les informations fournies à l'égard du développement de logiciel sécurisé et de l'application de mesures de chiffrement des données inactives et des données en transit ?				
8. Des mécanismes de recours sont-ils disponibles, et le cas échéant, dans quelle mesure sont-ils efficaces ?				

[2] Précité, note 5.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
PARTIE II – ÉVALUATION PROPRE AUX SOLUTIONS REPOSANT SUR L'IA ET L'APPRENTISSAGE AUTOMATIQUE				
9. Quels sont les risques liés à une défaillance technique de la solution Pandemic Tech ? Quels sont les risques liés à des résultats inexacts, à des ensembles de données pollués et à une utilisation abusive ?[2]				
Synthèse du principe · Toutes les mesures techniques et organisationnelles adoptées pour assurer la sécurité de la solution Pandemic Tech doivent notamment être synthétisées et évaluées.				
Principe 6 : Données ouvertes, concurrence loyale et propriété intellectuelle *Les entités responsables de projets qui développent, déploient ou utilisent des systèmes fondés sur des données et toute législation nationale réglementant une telle utilisation doivent promouvoir des cadres ouverts et décentralisés. Les entités responsables de projets qui développent, déploient ou utilisent la solution Pandemic Tech doivent prendre les mesures nécessaires pour protéger les droits sur les œuvres qui en résultent par le biais d'une application appropriée et dirigée des lois en vigueur relatives aux droits de propriété intellectuelle.* **Aperçu du principe** · L'entité responsable du projet doit évaluer comment la solution Pandemic Tech et ses données de sortie peuvent être utilisées dans une autre situation de pandémie ou par une autre entité responsable de projets. · Les entités responsables de projets doivent être autorisées à protéger les droits sur la solution Pandemic Tech. Toutefois, il convient de veiller à ne pas prendre de mesures qui constitueraient une surprotection, ce qui pourrait nuire à l'objectif ultime de la protection de la propriété intellectuelle.				
1. La solution Pandemic Tech est-elle ouverte ?				
2. Des restrictions relatives à l'utilisation sont-elles clairement rendues publiques (p. ex., dans le cas de solutions ouvertes) ?				
3. La solution Pandemic Tech offre-t-elle une bonne portabilité ?				
4. Quelle est l'étendue de l'interopérabilité avec des solutions technologiques offertes par d'autres fournisseurs ?				
5. Dans le cadre de l'élaboration de « cartes de degrés de sensibilité » ou de projets connexes, les données partagées sont-elles anonymisées ?				
6. Les données générées par la solution Pandemic Tech sont-elles réutilisables dans d'autres projets d'intérêt public (projets fondés sur des données pour le bien collectif) ?				
7. Quels sont les droits de propriété ou de propriété intellectuelle rattachés à la solution Pandemic Tech ?				
8. La solution Pandemic Tech soulève-t-elle des enjeux relatifs à des licences obligatoires et à des droits de brevet ?				
9. Les droits de propriété intellectuelle rattachés à la solution Pandemic Tech ont-ils été rendus publics (de manière à faire du code sous-jacent un programme ouvert) ?				
10. Par ailleurs, existe-t-il des obligations ou des attentes concernant la fourniture du code ou logiciel sous-jacent au public ou à des entités gouvernementales ? Le cas échéant, des mesures seront-elles prises afin que les entités responsables de projets soient rémunérées adéquatement pour leur apport ?				
Synthèse des principes · Synthétiser les droits et restrictions associés à l'utilisation de la solution Pandemic Tech.				

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
Principe 7 : Protection des données à caractère personnel *Les responsables de projets qui développent, déploient ou utilisent la solution PandemicTech et toute législation nationale portant sur une telle utilisation doivent s'efforcer de garantir la conformité des systèmes fondés sur des données aux normes et réglementations relatives à la protection des données à caractère personnel, en tenant compte des caractéristiques uniques de ces systèmes de l'évolution des normes sur la protection des données à caractère personnel.* **Aperçu du principe** L'entité responsable du projet doit envisager de mettre en œuvre des mesures de protection opérationnelles visant à protéger les données à caractère personnel, comme des principes de protection des données dès la conception, spécialement adaptées aux caractéristiques spécifiques de la solution Pandemic Tech déployée.				
1. Les principes de la nécessité, de la proportionnalité et de la minimisation des données sont-ils pleinement intégrés ?				
2. Quelles mesures de protection des données à caractère personnel ont-elles été mises en œuvre dans le cadre de la conception ?				
3. Des données à caractère personnel recueillies par la solution Pandemic Tech sont-elles destinées à être utilisées à des fins secondaires pendant ou après la pandémie ? Le cas échéant, l'utilisation secondaire de ces données est-elle compatible avec les fins initialement prévues ?				
4. Comment les transferts de données de la solution Pandemic Tech hors des frontières (européennes, nationales, régionales) sont-ils organisés ?				
5. Quelle est la base légale de l'entité responsable du projet pour traiter des données à caractère personnel ? Quelles sont les mesures prises par l'entité responsable du projet pour en assurer la conformité ?				
6. Quelles étaient les personnes concernées ? Quel type d'information a été recueilli sur elles ? Quelle est la portée des consentements obtenus ?				
7. Des enfants ou d'autres groupes vulnérables sont-ils concernés ? Ce type de traitement ou de failles de sécurité fait-il l'objet de préoccupations ?				
8. Quelle est la nature de la relation que l'entité responsable du projet entretient avec les personnes concernées ? De quelle part de contrôle disposeront-elles ? S'attendraient-elles à ce que l'on utilise leurs données de cette manière ?				
9. Des données sensibles ont-elles été recueillies ? Le cas échéant, des normes plus contraignantes sont-elles mises en application afin de protéger ce type de données ?				
10. Comment les données utilisées par la solution Pandemic Tech ont-elles été recueillies et stockées ? Ont-elles été transférées par des tiers ou seront-elles transférées à des tiers ? – Déterminer si les données ont fait l'objet d'un prétraitement avant l'analyse et si cela a pu influer sur l'exactitude et le caractère approprié des individus.				
11. Existe-t-il d'autres possibilités viables que l'utilisation de données à caractère personnel (p. ex., l'anonymisation de données de synthèse) ? Le cas échéant, quels sont les mécanismes et techniques appliqués pour empêcher une réidentification ?				
12. Déterminer si les données sont fournies par une personne (créées du fait de l'action d'une personne), et si : – Les données sont déclenchées (le fruit de l'action d'une personne qui donne lieu à une relation) – Les données sont transactionnelles (créées lorsqu'une personne participe à une transaction) – Les données sont publiées (créées lorsqu'une personne s'exprime de façon proactive)				

[3] Ibid.

Facteurs à prendre en compte aux fins de l'attribution de la cote de risque	Comment la solution prend en compte ces facteurs, le cas échéant	Cote de risque (Faible, Modéré, Élevé)	Mesures d'atténuation	Commentaire
13. Déterminer si les données sont observées (créées après qu'une personne a été observée et enregistrée), et si : – Les données sont issues d'un engagement (lorsqu'une personne sait qu'elle est observée à un moment précis) – Les données sont imprévues (lorsqu'une personne est au fait de la présence de capteurs, mais qu'elle ne sait pas vraiment qu'ils créent des données la concernant) – Les données sont passives (lorsqu'il est très difficile pour une personne de savoir qu'elle est observée et que des données découlant de cette observation sont créées)				
14. Déterminer si les données sont dérivées (créées de façon mécanique à partir d'autres données, devenant de nouveaux éléments de données relatifs à une personne), et si : – Les données sont fondées sur des calculs (création de nouveaux éléments de données par un processus arithmétique effectué sur des éléments numériques existants) – Les données sont fondées sur une notation (création de nouveaux éléments de données en classant des personnes dans un groupe en fonction d'attributs communs entre les membres du groupe)				
15. Déterminer si les données sont déduites (le produit d'un processus analytique axé sur la probabilité), et si : – Les données sont statistiques (le produit d'une caractérisation basée sur un processus statistique) – Les données sont de nature analytique avancée (le produit d'un processus analytique avancé)[3]				
16. Au-delà de la protection des données à caractère personnel des personnes concernées, la protection des données à caractère personnel d'un groupe identifié est-elle susceptible d'être compromise ?				
17. Existe-t-il des procédures pour l'examen de la conservation de données et pour la destruction de données utilisées par la solution Pandemic Tech ? Y a-t-il des mécanismes de surveillance en place				
18. La solution Pandemic Tech comporte-t-elle une fonctionnalité permettant à l'utilisateur de la « fermer » pendant une période limitée ?				
Synthèse du principe · Résumer la mesure dans laquelle l'entité responsable du projet adhère au principe de protection des données à caractère personnel et de la vie privée : – Personnes sur lesquelles portent les données – Catégories de données – Droits et exercice – Possibilité de conflit avec l'équipe Protection des renseignements personnels de groupes de personnes				

4. SOMMAIRE DE L'ÉVALUATION DES RISQUES

La présente section sert à décrire les risques identifiés dans le cadre de l'EIP ainsi que les mesures proposées pour atténuer et gérer ces risques. Il peut s'avérer utile de les mettre en rapport avec les principes susmentionnés pour bien justifier la pertinence de ces risques et des mesures proposées. Par souci d'efficience, documentez les risques conformément aux processus de gestion des risques de l'entité responsable du projet, plutôt que de tenter d'effectuer un processus distinct.

5. PLAN D'ACTION POUR L'ATTÉNUATION DES RISQUES

La présente section sert à décrire les mesures proposées pour atténuer et gérer les risques décrits précédemment. Dans certains cas, il peut être utile de catégoriser les mesures par secteur, notamment : **Gouvernance / Ressources humaines / Processus / Technologie**.

Veuillez fournir des précisions sur les stratégies proposées. Veuillez également indiquer la probabilité (faible, modérée ou élevée) que chaque risque se matérialise et la gravité de l'impact qu'il aurait alors sur les gens. Vous pouvez utiliser le modèle de tableau ci-après.

Tableau relatif à l'atténuation des risques

	Risque	Stratégie d'atténuation	Probabilité	Retombées
1.				
2.				
3.				
4.				
5.				

ANNEXE 3

TABLEAU DE COMPARAISON DE 11 INITIATIVES

Solution	Protocole de communication/ Application/ Portable	Gouvernement/ Secteur privé/ OBNL	Revue éthique/ AIPD/EIP	Centralisée/ Décentralisée/ Hybride	IA/AM ou non	GPS/ Bluetooth/ Autre	Auto-diagnostic/ Diagnostic confirmé
1 MILA – Application COVI	Application	Organismes à but non lucratif	EIP	Hybride : Principalement décentralisée avec des éléments centralisés	IA/AM	Initialement GPS/ subséquemment Bluetooth	Diagnostic confirmé/ Évaluation des risques développée par l'IA
2 ROBERT	Protocole	Gouvernement	Manifesto PEPP PT[1]	Hybride : Principalement centralisée avec des éléments décentralisés	Non	Bluetooth	En fonction de l'application (en principe, auto-diagnostic)
3 Corona-Datenspende	Application	Gouvernement	Non disponible	Centralisée	Non	Appareils connectés	s. o. (aucun diagnostic)
4 Apple/Google	Protocole	Secteur privé	Non disponible	Décentralisée	Non	Bluetooth	En cas de diagnostic de COVID-19, les utilisateurs doivent donner leur consentement pour partager leurs données du diagnostic sur le serveur.
5 DP-3T	Protocole	Gouvernement	AIPD	Hybride : Principalement décentralisée avec des éléments centralisés	Non	Bluetooth LE	Diagnostic confirmé
6 NHS	Application	Gouvernement	AIPD	Centralisée	Non	Bluetooth LE	Auto-diagnostic suivi d'une confirmation du diagnostic. Auto déclaré/ divulgation des données.
7 TraceTogether	Application	Gouvernement	AIPD	Hybride : Principalement décentralisée avec des éléments centralisés	Non	Bluetooth	Diagnostic confirmé
8 Coalition	Application	Organismes à but non lucratif	AIPD	Hybride : Principalement décentralisée avec des éléments centralisés	Non	Bluetooth	Auto-diagnostic
9 Aarogya Setu	Application	Gouvernement	Non disponible	Hybride : partiellement centralisée	Non	GPS, Bluetooth	Auto-diagnostic
10 Estimote[2]	Appareil portable et logiciel dorsal	Secteur privé	Aucune	Centralisée	Non	GPS, LTE, Bluetooth	Auto-diagnostic
11 TerraHub Credential Link	Application	Secteur privé	Non disponible	Hybride : Principalement décentralisée avec des éléments centralisés	Non	Chaîne de blocs	Possibilité d'auto-diagnostic et de diagnostic confirmé (en fonction des données téléchargées sur la plateforme)

	Données sur la santé publique	Utilisation limitée	Conservation limitée	Sécurité/ Fiabilité	Territoire (portée actuelle et proposée)	Interopérabilité
	Oui	Utilisation limitée à la COVID-19	Conservation limitée à la COVID-19	Cryptage Techniques différentielles de protection de la vie privée Pseudonymisation Vulnérabilité en raison du déploiement temporaire du GPS	Portée actuelle : Canada, mais potentiellement illimitée	Oui
	En fonction de l'application (en principe, non)	En fonction de l'application (en principe, limitée à la COVID-19)	En fonction de l'application (en principe, limitée à la COVID-19)	Pseudonymisation Cryptage	Premier et unique déploiement prévu en France ; portée potentiellement illimitée	En fonction de l'application
	Non	Limitée à la COVID-19 (traitement supplémentaire après anonymisation)	Limitée à la COVID-19 (traitement supplémentaire après anonymisation)	Pseudonymisation Cryptage	Allemagne (autres déploiements improbables)	Aucune
	Non	Utilisation limitée à la COVID-19	Conservation limitée à la COVID-19	Cryptage Suivi numérique des individus ayant été à proximité de personnes infectées	Sous réserve de mise en œuvre	Probable, mais sous réserve de mise en œuvre
	Non	Utilisation limitée à la COVID-19	Limitée à la COVID-19, mesures de protection liées à la capacité de conservation	Sensible au risque de piratage lié à la technologie BT LE (p. ex., conduite guerrière) Utilisation d'identifiants éphémères rotatifs (« EphID »)	Sous réserve de mise en œuvre à l'échelle nationale	Probable, mais sous réserve de mise en œuvre
	En principe, non. Importante mise en garde intégrée	En principe, à usage unique Mesures de protection intégrées insuffisantes Risque élevé que la solution soit utilisée à d'autres fins	En principe, mesures de protection limitées en matière de conservation, mais mesures de protection intégrées insuffisantes	Sensible au risque de piratage lié à la technologie BT LE (p. ex., conduite guerrière) Utilisation d'identifiants éphémères rotatifs (« Sonar ID »)	Portée actuelle : Île de Wight, mais portée proposée : R.-U. Portée limitée au R.-U.	Non
	Oui	Utilisation limitée à la COVID-19	Durée de conservation de 21 jours sur les appareils personnels	Cryptage Pseudonymisation Stockage des données d'identification à caractère non personnel Aucun accès sans le consentement	Singapour (adoptée également en Australie par l'intermédiaire de COVIDSafe) Les détenteurs d'un numéro de téléphone de Singapour ont accès à l'application aux É.-U. et au R.-U.	Non
	Non	Utilisation limitée à la COVID-19	Conservation limitée à la COVID-19	Cryptage	Portée générale	Oui
	Potentiellement, oui	Utilisation limitée à la COVID-19 et aux fins de recherche	Utilisation limitée à la COVID-19 et aux fins de recherche	Cryptage Dans certains cas, désidentification et anonymisation aux fins de recherche	Inde	Non
	Non	Solution entièrement programmable par l'entreprise qui la déploie Aucun contrôle en place Risque élevé que la solution soit utilisée à d'autres fins	Aucune donnée divulguée En fonction de l'entreprise qui la déploie	Même si les données sont dites anonymes lorsqu'elles sont transmises au serveur dorsal, aucune donnée concernant la sécurité ou la fiabilité de l'appareil portable, la transmission des données d'un appareil au serveur dorsal, ou le fonctionnement et le stockage des données sur le serveur dorsal n'a été divulguée.	Entreprise située en Pologne (avec des bureaux aux É.-U.), mais prévoit diffuser la solution à l'échelle mondiale	s. o.
	Potentiellement, oui	Initialement déployée à des fins de sécurité en milieu de travail, puis étendue à la COVID-19, mais sans s'y limiter. Une fois la pandémie sous contrôle, les fonctions liées à la COVID-19 seront mises hors service.	La durée de conservation est illimitée pour les données stockées sur la chaîne. La durée de conservation des données personnelles stockées hors de la chaîne dépendra de la politique de la base de données du tiers.	Cryptage des données inactives et des données en transit Technologies d'amélioration de la protection de la vie privée Utilisation de méthodes de contrôle qualité	Portée actuelle : Alberta, Canada ; mais potentiellement illimitée.	Oui

ANNEXE 4

RAPPORTS D'ÉTUDE PIA

Dans le cadre du projet PostCoviData mené par la Human Technology Foundation, les résumés des Rapports d'étude PIA reproduits dans cette annexe ont été préparés sur la base d'un examen des documents accessibles au public par les membres de l'**Association ITechLaw** qui sont cités comme contributeurs pour chacun des documents respectifs. Les contributeurs ont participé à ce projet à titre personnel. En conséquence, les points de vue exprimés dans les résumés des Rapports d'étude PIA ne reflètent pas ceux des cabinets d'avocats ou des autres entités auxquels ils peuvent être affiliés. Les contributeurs ont travaillé avec diligence pour s'assurer que les informations contenues dans les Rapports d'étude PIA sont exactes au moment de leur publication. L'éditeur recevra volontiers des informations qui l'aideront à rectifier toute erreur ou omission involontaire.

- COVI-APP (MILA)
- DP3T
- NHSX
- ROBERT
- CORONA-DATENSPENDE
- APPLE/GOOGLE
- TRACETOGETHER
- COALITION
- AAROGYA SETU
- ESTIMOTE
- TERRAHUB CREDENTIAL LINK

MILA – Institut québécois d'intelligence artificielle
Application COVI Canada
Rapport d'étude d'impact PostCoviData (« EIP »)

4 juin 2020

Comité d'évaluation ItechLaw
Charles Morgan, McCarthy Tétrault LLP
Manuel Morales, Université de Montréal
Allison Marchildon, Université de Sherbrooke

© ItechLaw Association 2020, CC-BY-SA

À lire en parallèle avec l'étude d'impact PostCoviData et le livre blanc sur l'application COVI Canada (« **app COVI** »).

FACTEURS JUSTIFIANT DE PROCÉDER À UNE ÉTUDE D'IMPACT

- L'application COVI Canada (« **app COVI** ») est une application mobile décentralisée de traçage de contacts et d'évaluation du risque qui a été développée par un consortium dirigé par l'Institut québécois d'intelligence artificielle (« **MILA** »).

- L'application est conçue pour le traçage des contacts entre les utilisateurs, de façon à évaluer leur risque d'infection par la COVID-19 et à leur fournir des recommandations sur leur comportement actuel ou à la suite de changements du niveau de risque. Elle vise également à fournir aux autorités gouvernementales des informations agrégées sur les risques de contagion afin de les aider à concevoir des réponses plus efficaces à la pandémie.

- Plutôt qu'une évaluation binaire (oui/non) à savoir si la personne a été en contact avec une autre personne ayant reçu un diagnostic de COVID 19, la solution d'intelligence artificielle (« IA »)/ apprentissage machine (« AM ») développée par MILA calcule la probabilité globale d'exposition des utilisateurs à la COVID-19 (le « score de risque »), sur la base des informations démographiques, sanitaires et comportementales fournies par l'utilisateur, des diagnostics officiels s'ils sont disponibles, et des scores de risque des autres utilisateurs du réseau. À notre connaissance, COVI est la seule application de traçage de contacts qui cherche à envoyer des messages de risque à plusieurs niveaux.

- Cette solution permet à l'application installée sur les appareils des utilisateurs d'envoyer et de recevoir des scores de risque grâce à un système de messagerie privée. Si des diagnostics officiels deviennent disponibles et qu'un utilisateur reçoit un résultat positif confirmé par les autorités de santé publique, les autres utilisateurs qui se sont trouvés à proximité de cet utilisateur seront contactés par messagerie privée. L'application enverra un message qui n'indique ni l'heure ni le lieu du contact, informant ces autres utilisateurs qu'ils courent un risque accru et leur proposant des mesures appropriées, comme d'être attentif à l'apparition de symptômes.

- L'application demande à l'utilisateur de fournir un état de santé, des conditions préexistantes et des paramètres démographiques au moyen d'un questionnaire d'auto-diagnostic. Elle combine ensuite ces informations avec le suivi par GPS et Bluetooth pour recommander des actions et des conseils personnalisés et non binaires. Elle utilise un algorithme d'apprentissage machine qui prédit à l'utilisateur des actions personnalisées en fonction des risques. Il s'agit également d'une plateforme permettant de partager des diagnostics de COVID-19 positifs confirmés dans le réseau de contacts afin de mettre à jour le niveau de risque et les recommandations pertinentes aux utilisateurs concernés. Grâce à la combinaison du GPS et du Bluetooth, des diagnostics positifs et d'un algorithme d'apprentissage machine, l'objectif est de modifier le comportement individuel pour isoler (confinement auto-imposé) les personnes à haut risque au fur et à mesure de l'apparition de nouveaux cas positifs

et que se dessine leur chemin de contagion de personne à personne.

- Le système repose sur des capacités hybrides décentralisées de stockage et d'analyse de données. Les données sont stockées en majeure partie sur les appareils mobiles des utilisateurs. Les informations recueillies par l'application ne seront accessibles qu'à la fiducie de données de MILA sous forme pseudonymisée afin de former et d'affiner son modèle d'évaluation des risques basé sur l'apprentissage machine, de comprendre par combien de personnes l'application a été adoptée et comment ses fonctionnalités sont utilisées, et de déterminer si les recommandations formulées ont un impact sur le score de risque d'un utilisateur. Des données dépersonnalisées et agrégées basées sur ces informations peuvent être fournies au gouvernement pour l'analyse épidémiologique et la planification stratégique. Les données de géolocalisation pour le traçage des contacts sont échangées par messagerie privée et protégées du traçage par un système de cryptage.

- Selon le livre blanc sur COVI, les ensembles de données pseudonymisées et de risques liés à la zone géographique nécessaires à la formation de modèles statistiques et épidémiologiques prédictifs seront stockées dans un serveur sécurisé dont l'accès sera limité à certains chercheurs en IA qui entraîneront ces modèles. Cette machine ne sera pas gérée par le gouvernement. MILA travaille actuellement à la création de COVI Canada, organisme sans but lucratif axé sur la gestion de ces données selon les normes les plus élevées de bonne gouvernance et dont l'unique objectif est de protéger la santé, le bien-être, la dignité et les renseignements personnels des Canadiens.

- Les personnes concernées seront des citoyens qui auront installé l'app COVI (initialement au Canada, principalement au Québec).

- **L'app COVI traitera les données sur la base du consentement ; son utilisation sera volontaire.**

- Principales exigences réglementaires : conformité avec les principales lois en matière de confidentialité et de protection des renseignements personnels dans les territoires où l'application est déployée. Au Canada, il s'agit de la *Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5* (« **LPRPDE** ») ; de la *Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P -39.1)* (« **LPRPSP du Québec** »), de la *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63 (« **LPRP de la Colombie-Britannique** ») ; de la *Personal Information Protection Act* (Alberta), S.A. 2003, c P -6.5 (« **LPRP de l'Alberta** »).

- Principales questions éthiques : confidentialité ; droit de ne pas être discriminé ; liberté de circulation ; transparence de la gouvernance ; besoin d'une instance d'évaluation éthique multi-disciplinaire et indépendante.

- L'app COVI sera utilisée pour créer un score de risque pour chaque personne, mais pas pour prendre des décisions à son sujet ; elle sera plutôt utilisée (de manière anonyme) pour fournir aux personnes des informations pouvant les aider à réduire les risques pour eux-mêmes et pour les autres.

- L'auditabilité doit encore être confirmée, mais **le code source sera ouvert** et rendu public pour examen. Devront aussi être divulguées de façon transparente la structure et la composition de l'équipe de gestion de l'OBNL qui opérera l'application et gérera les données.

- L'incidence du **traitement de données par l'app COVI est importante** — elle permettra aux citoyens qui ont des téléphones intelligents assez récents de comprendre le risque à savoir s'ils ont été en contact avec d'autres personnes infectées (ou potentiellement infectées) et de les retirer de la chaîne d'infection **en leur proposant de s'isoler et en leur recommandant des mesures pour atténuer le risque, y compris l'auto-isolement**.

CRITÈRE 1 : BUT ÉTHIQUE ET AVANTAGE POUR LA SOCIÉTÉ

- En général, l'application a pour but de contribuer à aplatir la courbe épidémiologique des épidémies locales de COVID-19 et à éviter de nouvelles éclosions en facilitant le traçage des contacts, tout en protégeant la vie privée.

- Elle est conçue pour être utilisée sur une base volontaire et ne repose pas sur le traçage de mouvements individuels, mais plutôt sur des informations de proximité avec d'autres utilisateurs.

- L'app COVI est pensée pour promouvoir l'intervention et l'autonomie humaines.

  – Les utilisateurs devront donner leur consentement à plusieurs occasions au cours du processus de flux des données, de façon à contrôler quelles informations sont recueillies et à qui elles sont divulguées.

  – En outre, un utilisateur peut supprimer l'application et ses données à tout moment (c'est-à-dire qu'il peut retirer son consentement). Lors de la suppression, l'algorithme est réentraîné et les données associées à cet utilisateur sont entièrement supprimées de l'application et des données agrégées fournies aux autorités de santé publique.

  – Plutôt qu'une évaluation binaire (oui/non) à savoir si la personne a été en contact avec une autre personne ayant reçu un diagnostic de COVID-19, la solution d'intelligence artificielle « IA »/apprentissage machine (« AM ») développée par MILA calcule la probabilité globale d'exposition des utilisateurs à la COVID-19 (le « **score de risque** »), sur la base des informations démographiques, sanitaires et comportementales fournies par l'utilisateur, des diagnostics officiels s'ils sont disponibles, et des scores de risque des autres utilisateurs du réseau.

  – Il existe des inquiétudes quant à la possibilité que les scores de risque numériques aient des conséquences négatives (comme de faire paniquer un utilisateur qui aurait un score élevé ou de fournir à des personnes abusives un « point de contrôle » pour surveiller le comportement de partenaires de vie). L'app COVI donnera plutôt de l'information et des recommandations en fonction de changements au score de risque. Cette approche vise à responsabiliser l'utilisateur, en le mettant en position d'adopter les comportements appropriés en fonction de son niveau de risque. Étant donné que le score de risque de l'utilisateur est lui-même partiellement fonction du score de risques d'autres personnes, le fait de fournir des recommandations plutôt qu'un score numérique ajoute une couche supplémentaire d'obfuscation, réduisant ainsi la possibilité de faire des inférences sur le score de risque d'autres utilisateurs.

  – Le bénéfice sociétal derrière le projet soulève également une préoccupation. Nous recommandons par conséquent la communication transparente des études entreprises incluant le nom des experts impliqués - en amont par les développeurs pour adresser et documenter l'efficacité, et les paramètres d'opérabilité, mais aussi pour identifier les enjeux éthiques et les bénéfices sociétaux.

  – Nous remarquons aussi le besoin d'établir un lien plus fort avec la santé publique pour assurer et renforcer les bénéfices sociétaux ainsi que l'acceptabilité sociale de l'application.

CRITÈRE 2 — RESPONSABILITÉ

- Les données pseudonymisées nécessaires à la formation de modèles statistiques et épidémiologiques prédictifs seront stockées dans un serveur sécurisé dont l'accès sera limité à certains chercheurs en IA qui entraîneront ces modèles.

- Cette machine ne sera pas gérée par le gouvernement. MILA travaille actuellement à la création d'une fiducie sans but lucratif, COVI Canada, pour le stockage des données.

- Selon le livre blanc sur COVI, COVI Canada aura des règles ouvertes sur sa gouvernance, un accès ouvert au code et aux modèles épidémiologiques agrégés, et serait continuellement surveillée par son conseil d'administration et des comités d'experts internes et soumise à des évaluations externes de groupes universitaires indépendants et de représentants gouvernementaux, pour veiller à ce qu'elle reste fidèle à sa mission. Le modèle complet de gouvernance de COVI Canada s'articule autour des valeurs de base de légitimité, de responsabilité, de transparence et d'efficacité. [...] La mission unique de COVI Canada qui est de soutenir les Canadiens dans leur combat contre la COVID-19 ainsi que sa nature d'organisme sans but lucratif garantissent que les données collectées ne seront jamais utilisées à des fins commerciales, ni vendues à des entreprises privées. Elles ne peuvent pas être utilisées à des fins de surveillance ou pour permettre aux gouvernements d'imposer une quarantaine. Les données sont toutes stockées au Canada et seront supprimées dès que la pandémie sera chose du passé.

- La création d'une structure OBNL qui gérerait l'application et les modèles prédictifs est prévue par les développeurs. Pour encadrer cette structure, nous recommandons la mise en place d'une infrastructure éthique indépendante. Notamment, la création d'un comité ou instance d'évaluation éthique multidisciplinaire et indépendante pour assurer un suivi du projet de la conception à la mise en oeuvre et s'occuper des questions éthiques au sein de l'OBNL. Cette instance indépendante pourrait par ailleurs mettre en place un processus de déclarations d'intérêts et de communication avec le public afin d'assurer la transparence quant à la composition de l'équipe de gestion de l'OBNL, aux liens de ses membres et ses sources de financement.

CRITÈRE 3 — TRANSPARENCE ET EXPLICABILITÉ

- Les utilisateurs seront des membres du grand public sans connaissance technique particulière.

- Selon le livre blanc sur COVI, pour veiller à ce que les utilisateurs comprennent bien les éléments clés des conditions générales et qu'ils ne se contentent pas de les accepter sans les lire, les conditions sont présentées selon une approche « progressive » à plusieurs niveaux, ce qui a semblé réaliser l'équilibre entre l'expérience utilisateur et la transparence du système. Par exemple, une couche supérieure graphique illustrant les implications en matière de vie privée peut être reliée à une deuxième couche un peu plus textuelle — celle-ci peut alors renvoyer à la section plus longue de la FAQ sur le site Web, qui à son tour renvoie les utilisateurs à la politique complète de protection de la vie privée.

- Selon le livre blanc sur COVI, on vérifie que les utilisateurs ont bien compris plutôt que de le tenir pour acquis : tout d'abord, nous appliquons l'analyse dans l'application pour estimer la compréhension des utilisateurs — par exemple, en examinant le taux d'utilisateurs qui décrochent aux différentes couches de divulgation des informations. Ensuite, nous soumettons à des questionnaires de compréhension dynamiques un échantillon aléatoire d'utilisateurs, ce qui nous permet de comprendre quelles informations ont été ou non internalisées. Enfin, les outils de divulgation sont révisés régulièrement en fonction des rétroactions sur ces mesures, afin de s'assurer qu'ils répondent au mieux au comportement réel des utilisateurs.

- Les données de sortie du modèle peuvent être expliquées et les décisions, vérifiées. L'utilisateur ne reçoit pas d'informations spécifiques sur le calcul de l'évaluation des risques. L'utilisateur ne recevra que des recommandations et des conseils personnalisés qui seront mis à jour au fur et à mesure que de nouvelles informations seront disponibles.

- MILA mettra en place une page Web pour l'application (où les utilisateurs pourront trouver la politique de protection des renseignements personnels), où il sera expliqué comment soumettre une plainte à propos du traitement par MILA des informations personnelles relativement à l'application.

CRITÈRE 4 — ÉQUITÉ ET NON-DISCRIMINATION

- Les données utilisées seront une combinaison de données communiquées par les utilisateurs et de données générées automatiquement par les appareils des utilisateurs. La mesure dans laquelle les données seront « représentatives » dépendra

du nombre d'utilisateurs et de leurs données démographiques et géographiques relatives. On estime qu'il faudra un taux d'adoption de 60 % de l'app COVI dans la population pour assurer l'efficacité et la précision de sa composante de traçage de contacts. Pour l'aspect IA (données agrégées, modèles épidémiologiques, etc.), MILA estime que le pourcentage minimal requis est beaucoup plus bas, soit environ 10 %.

- Les groupes marginalisés sont à la fois les plus susceptibles d'être affectés et les moins susceptibles d'avoir accès à un outil comme COVI et donc de l'utiliser. C'est pourquoi MILA a indiqué que la composition de la structure de gouvernance de la fiducie de données COVI Canada sera soumise à de fortes pratiques d'inclusion (c'est-à-dire représentation de la société civile, y compris les groupes vulnérables). En outre, l'algorithme sera formé pour garantir l'absence de biais et sera soumis à une étude d'impact algorithmique indépendante, notamment sur le front de la diversité et de l'inclusion.

CRITÈRE 5 — SÉCURITÉ ET FIABILITÉ

- Comme il s'agit d'un réseau de messagerie privé qui demande aux utilisateurs d'entrer directement des informations démographiques, leur condition de santé et leurs symptômes, l'exactitude de l'évaluation des risques (et donc des mesures recommandées) ne peut être garantie si les utilisateurs entrent de fausses données à leur sujet. Ces fausses données peuvent avoir une incidence sur le score de risques propagé par la solution, mais à moins qu'un grand nombre d'utilisateurs ne soient malhonnêtes (en proportion de l'ensemble des utilisateurs), cette incidence ne sera pas significative.

- Si un utilisateur reçoit un diagnostic officiel, un jeton spécial ou un mot de passe unique lui sera remis par l'autorité de santé publique. En d'autres termes, ces diagnostics seront validés par les autorités de santé publique et ne seront pas seulement autodéclarés.

- **Risques résiduels :** les développeurs ont identifié plusieurs scénarios d'attaque préméditée comme des risques résiduels inhérents à tout système de traçage automatique de contacts dans lequel il n'y a pas de restriction à la création de comptes.

- Nous sommes d'avis que pour que ces risques se concrétisent, il faudra **un savoir-faire technologique et une intention malveillante**.

- Les points ci-dessus doivent être considérés dans le contexte de l'utilisation de l'application par le grand public. Les niveaux de connaissances technologiques doivent être considérés comme faibles. Les utilisateurs traiteront l'application comme n'importe quelle autre sur leur téléphone. Toutefois, des niveaux de confiance supplémentaires peuvent être présumés, car l'application sera diffusée avec la participation et l'approbation des autorités de santé publique. Les attentes en matière de sécurité, de protection contre les risques et de fiabilité de l'application seront donc extrêmement élevées. En outre, il doit être absolument clair que l'application n'est pas un dispositif médical et (malgré les notifications et les recommandations) ne fournit ni ne remplace une assistance médicale. **Nous sommes donc préoccupés par le risque de décalage entre les niveaux réels de sécurité et de fiabilité et les attentes du public.**

- **Notre recommandation est qu'un programme de sensibilisation et d'éducation du public soit mis en œuvre** d'une manière adaptée au large spectre de la consommation publique.

CRITÈRE 6 — DONNÉES OUVERTES, CONCURRENCE LOYALE ET PROPRIÉTÉ INTELLECTUELLE

- La solution a été conçue pour être interopérable à l'échelle internationale.

- La solution sera offerte dans le cadre d'une licence de code source ouvert. Le modèle de licence est encore à déterminer.

CRITÈRE 7 — CONFIDENTIALITÉ

- La protection des renseignements personnels dès la conception fait partie de l'architecture de l'app COVI.

- Les données pseudonymisées seront transférées à la fiducie de données COVI Canada pour évaluation du score de risque.

- Selon le livre blanc sur COVI, afin d'améliorer la protection des renseignements personnels, les niveaux de risque sont quantifiés selon une précision sur 4 bits avant d'être échangés:.

- Lorsqu'un téléphone envoie un message à un autre téléphone via les serveurs cryptographiques, le destinataire ne sait pas de quel téléphone (ni le numéro de téléphone, ni l'adresse IP) provient le message. Afin de fournir une protection supplémentaire contre la stigmatisation, ces messages sont envoyés avec un délai aléatoire pouvant aller jusqu'à un jour.

- Les informations recueillies par l'application ne seront accessibles qu'à la fiducie de données de COVI Canada sous forme pseudonymisée afin de former et d'affiner son modèle d'évaluation des risques basé sur l'apprentissage machine, de comprendre par combien de personnes l'application a été adoptée et comment ses fonctionnalités sont utilisées, et de déterminer si les recommandations formulées ont un impact sur le score de risque d'un utilisateur. Des données dépersonnalisées et agrégées basées sur ces informations peuvent être fournies au gouvernement pour l'analyse épidémiologique et la planification stratégique. Les données de géolocalisation pour le traçage des contacts sont échangées par messagerie privée et protégées du traçage par un système de cryptage.

- Les données de géolocalisation et d'horodatage nécessaires pour le traçage des contacts seront cryptées localement au repos sur le téléphone (comme toutes les données recueillies par l'application), hachées à l'aide d'une fonction de hachage unidirectionnelle dès leur collecte, et les informations originales seront rejetées. Des méthodes d'obfuscation supplémentaires seront déployées, dès le lancement ou aussi rapidement que possible afin de limiter davantage les possibilités de réidentification des personnes à partir des traces de contact, que ce soit par les utilisateurs du système ou par les acteurs gouvernementaux.

- Les données recueillies, en majeure partie, seront régulièrement supprimées, comme suit :

  – Les données sur les téléphones des utilisateurs seront supprimées au plus tard 30 jours après leur collecte.

  – Les données utilisées pour entraîner l'algorithme seront supprimées au plus tard 90 jours après leur collecte.

  – Toutes les données seront supprimées lorsque la pandémie sera terminée.

Consortium DP-3T
DP-3T – Étude d'impact PostCoviData (« EIP »)
Sommaire des risques (principales constatations)

9 mai 2020

Comité d'évaluation d'ItechLaw
John Buyers, Osborne Clarke LLP
Trish Shaw, Beyond Reach
Nikhil Narendran, Trilegal
Lára Herborg Ólafsdóttir, Lex
Marco Galli, Gattai, Minoli, Agostinelli Partners Studio Legale
Rheia Khalaf, Université de Montréal, directrice, Recherche collaborative et Partenariats
Manuel Morales, Université de Montréal, professeur agrégé

© ItechLaw Association 2020, CC-BY-SA

À lire en parallèle avec l'EIP principale de DP-3T.

FACTEURS JUSTIFIANT DE PROCÉDER À UNE ÉTUDE D'IMPACT

- DP-3T est un protocole décentralisé destiné à une application de traçage des contacts hébergée sur les téléphones intelligents utilisant le système d'exploitation de Google (Android) ou d'Apple (IOS), et conçu pour faciliter le traçage de contacts dans le grand public. Il s'appuie sur une architecture pouvant être déployée à l'échelle internationale.

- L'évaluation des risques liés au protocole DP-3T est conditionnelle à l'implantation de la technologie à l'échelle nationale. Ainsi, le contexte juridique des pays qui adoptent le protocole peut varier, notamment en ce qui a trait aux règles de droit générales. À l'heure actuelle, DP-3T vise principalement les pays de l'Union européenne (UE) et européens (y compris les pays non membres de l'UE, comme le Royaume-Uni et la Norvège), qui se sont tous dotés de principes juridiques et démocratiques avancés, de lois en matière de protection des données cohérentes et bien établies et de lois sur la prévention de la discrimination. Les risques liés aux pays qui ne font pas partie de cette cohorte ne pourront pas être quantifiés tant que nous ne disposerons pas d'informations supplémentaires sur le contexte législatif et géopolitique de ces pays.

- La protection des données (RGPD et lois connexes, comme la directive relative à la vie privée et aux communications électroniques (ePrivacy Directive)), les lois applicables à l'utilisation des réseaux de télécommunications, les lois applicables à la protection des renseignements personnels et à la surveillance individuelle et de masse devront toutes être prises en compte aux fins de l'utilisation des applications reposant sur le protocole DP-3T.

- Les principales préoccupations éthiques relatives à l'utilisation des applications reposant sur le protocole DP-3T comprennent la protection des renseignements personnels, le droit de ne pas faire l'objet de discrimination, la liberté de mouvement, l'autonomie humaine, l'intervention humaine, la prévention des préjudices, les nouvelles formes de discrimination associées à la possession ou à l'absence de possession de l'application (qui ne sont pas nécessairement couvertes par les lois existantes sur l'équité), l'impact sociétal sur la confiance (du fournisseur et des co-utilisateurs) et le droit qu'une inférence ne puisse être faite à l'égard d'une personne ou d'un groupe de personnes.

- DP-3T ne repose pas sur l'IA ou l'apprentissage machine. Nous nous attendons néanmoins à ce que le déploiement de solutions décentralisées à l'échelle nationale comporte un certain degré de décision automatisée, en vertu de l'article 22 du RGPD.

- Les personnes concernées seront des citoyens ayant choisi d'utiliser l'application DP-3T. Les types de données sont des paquets de données pseudo-randomisées au moyen d'identifiants éphémères de la technologie BT LE (Bluetooth Low Energy) générés par les téléphones mobiles. Les données

utilisées peuvent être, dans des cas très limités (en particulier dans le modèle d'exploitation séparé décentralisé proposé dans le livre blanc intitulé « DP-3T White Paper Design 1 »), des données pseudonymisées reconstituées.

- Bien que l'information communiquée par le système de notification lorsqu'une personne présume elle-même qu'elle est infectée ne contienne aucune donnée sur la santé, la notification peut éventuellement être considérée comme une donnée sur la santé ou comme une donnée induite sur la santé, étant donné que seules les données provenant de personnes déclarées positives à la COVID-19, dont le diagnostic a été confirmé par un professionnel de la santé, sont téléversées dans le serveur dorsal.

- DP-3T s'explique clairement — la solution n'est pas opaque, étant donné qu'elle repose sur la communication conventionnelle au moyen de la technologie BT LE entre des appareils mobiles. L'auditabilité doit encore être confirmée, mais le code source sera ouvert et rendu public pour examen.

- Le traitement de données au moyen de l'application DP-3T a une incidence importante, car il permettra aux citoyens de savoir s'ils ont été en contact avec d'autres personnes infectées et d'interrompre la chaîne d'infection en s'auto-isolant. Bref, le traitement permettra aux pays de mieux gérer et atténuer l'impact de leur épidémie locale de COVID 19.

CRITÈRE 1 – BUT ÉTHIQUE ET AVANTAGE POUR LA SOCIÉTÉ

- L'application DP-3T, telle qu'elle a été conceptualisée, peut être considérée comme étant compatible avec les principes d'intervention et d'autonomie humaine, puisqu'elle a été conçue pour que la participation se fasse sur une base volontaire. Toutefois, cela dépendra de la mise en œuvre au niveau national.

- Même si la conception de DP-3T est compatible avec les principes d'intervention et d'autonomie humaines, nous recommandons l'élaboration de règles nationales de mise en œuvre pour favoriser l'intervention et l'autonomie humaines et le respect des droits fondamentaux. Le cadre législatif actuel qui s'applique à l'utilisation de telles applications se penche avant tout sur l'utilisation des appareils de télécommunications, ce qui ne protège pas le citoyen. À cet égard, nous recommandons au lecteur de se reporter au projet de loi intitulé *Coronavirus Safeguards Bill*, qui a été suggéré à titre de mesure de protection au Royaume-Uni.

- Nous recommandons que des mesures de protection additionnelles soient adoptées en ce qui a trait à la suppression des données. Selon le protocole DP-3T proposé actuellement, les données doivent être supprimées des serveurs après 14 jours, et la solution va se décomposer elle-même lorsqu'elle ne sera plus requise et que les utilisateurs cesseront de téléverser leurs données dans le serveur Autorisation, ou cesseront de l'utiliser. Nous proposons d'ajouter une disposition d'extinction en vertu de laquelle les données seront automatiquement supprimées lorsqu'un organisme externe (comme l'OMS) déclarera la fin de la pandémie.

- Nous recommandons que toute application DP-3T soit contractuellement conforme aux conditions d'utilisation standards de l'App Store d'Apple ou du Play Store de Google. Ces conditions comprennent des conditions distinctes relatives à la protection des données personnelles (le Play Store de Google fait entre autres référence à la politique de confidentialité de Google ; se reporter à la rubrique 9 de ces conditions ; se reporter également à la rubrique 5.1 du contrat de développeur d'Apple). Ces conditions peuvent avoir une incidence considérable sur le traitement des données personnelles par l'application DP-3T, et le compromettre.

- Le risque principal que présente cette application (comme toute application de traçage de contacts ou de proximité) est qu'elle peut être utilisée à d'autres fins après la pandémie (comme à des fins de surveillance par l'État). Le consortium DP-3T a fait preuve d'une très grande prudence (voire de méticulosité) pour faire en sorte que ce risque ne se matérialise pas pour DP-3T, notamment en prenant des mesures de conception particulières importantes dans l'élaboration de l'architecture DP-3T afin de conserver une structure décentralisée et de réduire au minimum les cas où les données personnelles sont utilisées ou peuvent être inférées.

- L'utilisation d'applications comme DP-3T offre des avantages indéniables pour le public. L'utilisation de l'application pourrait permettre à des États d'aplatir la courbe de l'épidémie locale de COVID 19. Il se pourrait que le niveau de granularité du traçage de contacts et des observations améliore de façon générale la science de l'épidémiologie. Ces informations pourraient aider les scientifiques à comprendre le graphique de proximité d'un utilisateur infecté en fournissant des précisions sur son interaction avec d'autres personnes et sur la transmission de l'infection qui en a découlé.

- Nous continuons d'être préoccupés par la possibilité que ces solutions technologiques donnent lieu à des comportements de « masse » indésirables dans la société, ce qui se traduirait par un biais d'automatisation (confiance inconditionnelle dans les résultats fournis par l'application), faussant ainsi la confiance à une extrémité et entraînant l'ostracisation des personnes les unes par rapport aux autres. Ces comportements peuvent bien sûr toucher les personnes infectées, mais peuvent également toucher les personnes qui ne possèdent pas de téléphone intelligent et qui sont donc « privés de leurs droits ».

CRITÈRE 2 — RESPONSABILITÉ

- Comme il a été mentionné précédemment, l'évaluation des risques liés au protocole DP-3T dépend de la mise en œuvre de la technologie à l'échelle nationale, qui peut avoir une incidence considérable sur l'évaluation plus large des risques liés à la solution (par exemple, en imposant des installations obligatoires ou des quarantaines obligatoires après une notification positive à la COVID 19). Nous ne sommes pas en mesure de faire des recommandations définitives en l'absence de telles mises en œuvre, mais nous avons formulé des observations sommaires sur la base de notre connaissance actuelle qui pourraient avoir une incidence sur ces mises en œuvre.

- Nous recommandons que le consortium DP-3T publie un cadre de règles nationales standards auxquelles l'utilisation de DP-3T serait assujettie, et qui pourraient servir de lignes directrices pour assurer la coopération internationale entre les gouvernements, la cohérence de l'utilisation et de l'application à l'échelle nationale et l'optimisation de l'interopérabilité entre les pays. Ces règles nationales standards devraient permettre à tous les citoyens de corriger les erreurs contenues dans leurs données qui sont conservées sur le serveur dorsal de DP-3T.

- Les dépendances envers des tiers pourraient également nuire considérablement à la responsabilité à l'égard de la solution. À cet égard, nous devons identifier les principaux fournisseurs de plateforme de système d'exploitation : Apple et Google. Nous recommandons que ces fournisseurs soient tenus de réaliser des analyses d'impact relatives à la protection des données distinctes et accessibles au public et de fournir un engagement irrévocable (ou autre engagement juridiquement exécutoire similaire) de conformité aux règles nationales relatives au traçage dans le cadre de la pandémie de COVID 19. Ces engagements exigeront non seulement la conformité à des cadres reposant sur des règles nationales, mais également de la transparence pour permettre de réduire au minimum (et de corriger) les erreurs contenues dans les solutions technologiques de chaque plateforme.

CRITÈRE 3 — TRANSPARENCE ET EXPLICABILITÉ

- Nous sommes convaincus que l'exploitation du système en termes de catégories de données et de fonctionnalité est clairement définie dans le livre blanc et la documentation connexe. Le serveur dorsal et le serveur Autorisation devraient être pleinement auditables, sous réserve que l'accès soit fourni par les organismes locaux chargés de la mise en œuvre. Nous remarquons que ce système n'est pas centralisé, mais plutôt hautement décentralisé. Les données locales détenues sur les téléphones intelligents ne seront pas visées par la portée de l'inspection et de l'audit, sauf si l'accès à celles-ci est accordé (ou si une ordonnance du tribunal est demandée).

- Le système DP-3T est sensible aux risques liés à la technologie Bluetooth LE et à d'autres cyber-risques propres à cette technologie. Ces risques ne sont pas uniques au DP-3T, mais sont des risques génériques propres aux solutions décentralisées de cette nature. Nous énumérons certains de ces risques ci-après, dans le contexte du critère 5 (Sécurité et fiabilité) qui suit. Selon nous, la documentation contient peu d'informations permettant de présumer que le système DP-3T est plus robuste que tout autre système reposant sur la technologie BT LE.

CRITÈRE 4 — ÉQUITÉ ET NON-DISCRIMINATION

- Comme il a été mentionné précédemment, l'évaluation des risques liés au protocole DP-3T dépend de la mise en œuvre de la technologie à l'échelle nationale, qui peut avoir une incidence considérable sur l'évaluation plus large des risques liés à la solution (par exemple, en imposant des installations obligatoires ou des quarantaines obligatoires après une notification positive à la COVID 19). Nous ne sommes pas en mesure de faire des recommandations définitives en l'absence de telles mises en œuvre, mais nous avons formulé des observations sommaires sur la base de notre connaissance actuelle qui pourraient avoir une incidence sur ces mises en œuvre.

- L'application DP-3T est conçue de manière à ce que la participation se fasse sur une base volontaire. Nous sommes toutefois préoccupés par la possibilité qu'un segment de la population nationale (près de 40 % des personnes âgées de plus de 65 ans et de celles âgées de moins de 16 ans) puisse ne pas pouvoir participer pour la seule raison qu'ils n'ont pas accès à un appareil intelligent ou n'en possèdent pas un.

- Nous avons déjà indiqué que l'application DP-3T (comme d'autres solutions similaires) pourrait donner lieu à des comportements de « masse » indésirables dans la société, ce qui se traduirait par un biais d'automatisation (confiance inconditionnelle dans les résultats fournis par l'application), faussant ainsi la confiance à une extrémité et entraînant l'ostracisation des personnes les unes par rapport aux autres.

- Nous sommes d'avis qu'il faudrait un système bien établi de redressement des faux positifs et des faux négatifs, ainsi que des risques de réidentification, des risques de colocalisation et des risques liés aux variables proxy. Comme nous l'avons mentionné dans le critère 2, nous recommandons que le consortium DP-3T publie un cadre de règles nationales standards auxquelles l'utilisation de DP-3T serait assujettie et qui pourraient servir de lignes directrices pour assurer la coopération internationale entre les gouvernements, la cohérence de l'utilisation et de l'application à l'échelle nationale et l'optimisation de l'interopérabilité entre les pays. Ces règles nationales standards devraient permettre à tous les citoyens de corriger les erreurs contenues dans leurs données qui sont conservées sur le serveur dorsal de DP-3T.

CRITÈRE 5 — SÉCURITÉ ET FIABILITÉ

- Tous les systèmes de traçage de proximité qui avisent les utilisateurs qu'ils sont à risque permettent à un adversaire motivé d'identifier la personne infectée (que ce soit en raison de comptes multiples, d'un enregistrement manuel, de délais d'enregistrement ou d'identification (intervalles de temps), ainsi que d'identification par photo ou vidéo). Par ailleurs, Il existe des faiblesses inhérentes à la technologie Bluetooth Low Energy qui peuvent être exploitées à des degrés divers de sophistication, comme l'injection de bruit, le traçage d'utilisateurs utilisant des projections orthogonales du traçage de contacts (p. ex. adresses MAC), la conduite guerrière et le vol de cellulaires.

- Selon nous, ces risques dépendent de l'intervention de spécialistes de la technologie et d'acteurs malveillants agissant dans l'intention de nuire. Le protocole DP-3T cherche à protéger le plus possible les renseignements personnels et à réduire au minimum les risques de réidentification (notamment dans le protocole de conception 2). Comme il a été mentionné au critère 3 qui précède, la documentation contient peu d'informations permettant de présumer que le système DP-3T est plus robuste que tout autre système reposant sur la technologie BT LE.

- Les points ci-dessus doivent être considérés dans le contexte de l'utilisation de l'application par le grand public. Les niveaux de connaissances technologiques doivent être considérés comme faibles. Les utilisateurs traiteront l'application comme n'importe quelle autre sur leur téléphone. Toutefois, des niveaux de confiance supplémentaires peuvent être présumés (en fonction de la culture), car l'application sera diffusée par les autorités nationales de santé publique (et les États). Les attentes en matière de sécurité, de protection contre les risques et de fiabilité de l'application seront donc extrêmement élevées. Nous sommes donc préoccupés par le risque de décalage entre les niveaux réels de sécurité et de fiabilité et les attentes du public.

- Nous recommandons qu'un programme de sensibilisation et de formation du public soit mis en place en relation avec la mise en œuvre du DP-3T dans chaque pays. À cet égard, une bande dessinée explicative en plusieurs langues peut être consultée sur une autre page Web GitHub publiée par le consortium DP-3T pour faciliter la participation du public.

CRITÈRE 6 — DONNÉES OUVERTES, CONCURRENCE LOYALE ET PROPRIÉTÉ INTELLECTUELLE

- Comme il a été mentionné précédemment, l'application DP-3T a été diffusée comme source ouverte. Les catégories de données sont des identités éphémères compactes pouvant être transmises au moyen des protocoles de la technologie BT LE. La publication complète a supplanté l'architecture système pour permettre cette portabilité. Compte tenu de la nécessité d'évaluer la mise en œuvre actuelle de DP-3T à l'échelle nationale, nous sommes dans l'incapacité d'examiner les normes d'interopérabilité actuelles.

- À la lecture de l'analyse d'impact relative à la protection des données distincte, nous comprenons que les données sur la localisation peuvent être traitées aux seules fins de permettre à l'application d'interagir avec des applications similaires dans d'autres pays. Nous ne savons pas si cet énoncé se rapporte à la mise en œuvre dans certains pays du système ou à d'autres données de contrôle du traçage décentralisé. D'autres évaluations techniques sont nécessaires pour évaluer cette capacité, et pour comprendre la mesure dans laquelle les données doivent être partagées entre les applications de traçage centralisées et décentralisées.

- À ce jour, en ce qui a trait au partage élargi de données, le protocole DP-3T ne prévoit pas, pour des raisons de protection des renseignements personnels, le partage de graphiques de proximité avec les épidémiologistes, bien que nous notions que cette fonctionnalité pourrait être activée dans des versions ultérieures.

- La nature de source ouverte de la solution DP-3T est confirmée par le fait que la licence pour la solution a été obtenue en vertu du cadre d'octroi de licences en source ouverte MPL 2.0. Le cadre MPL 2.0 est une simple licence de partage à l'identique qui encourage les personnes qui contribuent à partager leurs modifications au code, tout en leur permettant de combiner leur propre code avec les codes assujettis à d'autres licences (en source ouverte ou exclusifs), avec des restrictions minimales. Compte tenu de ce contexte, nous ne prévoyons pas qu'il y aura des risques complexes liés à la propriété intellectuelle, bien que nous soyons tenus de signaler les dépendances du protocole à l'égard des technologies exclusives, comme le système d'exploitation IOS d'Apple ou Android de Google. Dans une moindre mesure, nous voulons également mentionner que la technologie BT LE est elle aussi une technologie brevetée.

CRITÈRE 7 — PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

- Nos recommandations sont conformes à l'analyse d'impact relative à la protection des données distincte réalisée par EPFL (Edouard Bugnion) et id est avocats Sàrl (Michel Jaccard et Alexandre Jotterand), version 1.0, publiée le 1er mai 2020.

- En général, nous considérons que les données personnelles peuvent être traitées dans le cadre du système de façon limitée. Même dans un modèle déconnecté (voir le modèle 2 présenté dans le livre blanc), il est possible d'utiliser des moyens indirects pour corréler et confirmer des éléments de données personnelles suffisamment pour identifier des personnes, et ce sera certainement le cas lorsque le consentement aura été obtenu de téléverser des données sur des personnes infectées sur un serveur dorsal. Même si, dans la plupart des cas, la demande dans le cadre de la cause ***Breyer*** auprès de la Cour européenne de justice ne peut être satisfaite, nous sommes entièrement d'accord avec les auteurs de l'analyse d'impact relative à la protection des données qu'une approche conservatrice doit être adoptée et que la solution doit être considérée comme si elle permettait de traiter des données personnelles.

- Dans le contexte du deuxième point du critère 7, nous pensons également que ces données personnelles pourraient aussi contenir des données potentiellement sensibles (comme des données sur la santé). Bien que l'information communiquée par le système de notification lorsqu'une personne présume elle-même qu'elle est infectée ne contient aucune donnée sur la santé, la notification peut éventuellement être considérée comme une donnée sur la santé ou comme une donnée induite sur la santé, étant donné que seules les données provenant de personnes déclarées positives à la COVID-19, dont le diagnostic a été confirmé par un professionnel de la santé, sont téléversées dans le serveur dorsal.

Royaume-Uni : Application COVID19 du NHSx
Application COaVID19 du NHSx : Rapport d'étude d'impact PostCoviData (« EIP ») Sommaire des risques (principales constatations)

16 mai 2020

Comité d'évaluation d'ItechLaw
John Buyers, Osborne Clarke LLP
Patricia Shaw, Beyond Reach Consulting Limited

© ItechLaw Association 2020, CC-BY-SA

À lire en parallèle avec l'EIP principale pour l'application COVID19 du NHSx (« **application du NHSx** »).

FACTEURS JUSTIFIANT DE PROCÉDER À UNE ÉTUDE D'IMPACT

- Au moment de rédiger ce rapport, l'application du NHSx est en **test bêta** dans l'île de Wight (petite île au sud de l'Angleterre faisant partie des îles Britanniques). L'application du NHSx utilise un modèle centralisé (plutôt qu'un modèle décentralisé) pour le traçage de proximité – voir le diagramme ci-après. Elle est fondée sur une communication conventionnelle BT LE entre appareils mobiles. Le but est de simplifier et d'accélérer le processus d'identification des gens qui ont été en contact avec une personne testée positive au virus SARS-CoV-2.

- L'application du NHSx **repose sur l'auto-diagnostic des utilisateurs (confirmé ou non)**. Elle utilise des informations sur les rencontres de proximité (l'ID transmise, c'est-à-dire l'ID Sonar cryptée, ainsi qu'un horodatage de la rencontre et des informations sur l'intensité du signal radio) téléversées par les utilisateurs lorsqu'ils ont a) posé un auto-diagnostic d'infection (fondé sur l'apparition de symptômes évalués par l'outil) OU b) des résultats confirmés qu'ils ont été testés positifs au virus. Les informations fournies doivent révéler au serveur sonar dorsal centralisé les appareils qui se trouvent à proximité les uns des autres, ainsi que la durée et la distance de cette proximité.

- Dans le cadre de l'auto-diagnostic, l'application permet à l'utilisateur de demander un numéro de référence à usage unique du serveur sonar dorsal. Ce numéro est alors présenté à l'utilisateur via l'application. Il s'agit d'un identifiant unique qui peut être utilisé pour demander un test COVID-19 et pour interagir avec des **opérateurs humains** dans un centre d'appel dédié.

- Le système utilise un modèle centralisé géré par une autorité gouvernementale qui a demandé à ce que les futures versions de l'application offrent aux utilisateurs la possibilité de donner des données pour la recherche. Il y a donc un **plus grand risque** :

  – de détournement des fonctionnalités ou du mandat ;

  – d'utilisation d'informations d'une manière qui, sans être techniquement illégale, pourrait être considérée comme portant atteinte à la vie privée, comme la surveillance des interactions sociales/les graphiques de contact ;

  – que l'autorité gouvernementale puisse établir des liens entre les informations obtenues directement par l'application du NHSx et d'autres données qu'elle détient directement ou auxquelles elle a accès indirectement (comme les dossiers du service national de santé, des dossiers de géolocalisation des fournisseurs de téléphonie mobile, de l'information de fournisseurs d'interfaces de programmation ou de système d'exploitation, etc.) ce qui faciliterait la ré-identification des données ;

- qu'apparaissent de nouvelles formes de discrimination ou de stigmatisation en raison de la pression exercée par les autorités/les responsables civils qui évoqueraient le « devoir de citoyen » pour exiger, par exemple, le téléchargement de l'application avant de retourner au travail ;

- de cyberattaques puisqu'une base de données centralisée est susceptible d'être vue comme un « pot de miel ».

- Bien que le gouvernement britannique doive se conformer aux lois existantes pour protéger les droits de la personne, protéger les données personnelles et prévenir la discrimination (entre autres lois applicables à l'utilisation des réseaux de télécommunications, à la protection de la vie privée et à la surveillance individuelle et de masse), les juristes et les universitaires ont souligné **la nécessité de lois supplémentaires**. Il est proposé qu'une loi supplémentaire prévoie des mesures de protection ou de gestion par rapport à d'éventuelles utilisations abusives des systèmes par des acteurs malveillants ou à des détournements de mandat et pour empêcher qu'apparaissent de nouvelles formes de discrimination (dans la mesure où ces éléments ne sont pas déjà couverts par le RGPD, la directive relative à la vie privée et aux communications électroniques, la Equality Act, la *Digital Economy Act 2017*, la Computer Misuse Act, la *Investigatory Powers Act 2016*. Par exemple, il y a de l'incertitude à savoir dans quelle mesure **l'article 61A, partie 3 de la *Investigatory Powers Act 2016*** (qui permet de suivre sans préavis les personnes ayant reçu un diagnostic de coronavirus ou en présentant des symptômes), permettra à ces autorités d'enquête d'avoir accès aux informations en transit ou en stockage. À cette fin, nous commentons le projet de loi **Coronavirus (Safeguards) Bill 2020**.

- L'architecture proposée ne serait pas compatible avec la future interface de programmation d'applications d'Apple (iOS) et de Google (Android), et pourrait donc poser des **problèmes lors de son déploiement sur les téléphones intelligents d'Apple**. En raison de son architecture centralisée, l'application du NHSx ne pourra probablement pas être déployée à l'échelle internationale et ne **démontre pas actuellement son interopérabilité** avec d'autres protocoles, tels que le DP-3T

- En raison des préoccupations relatives à la protection de la vie privée et des éventuels problèmes technologiques liés à la capacité « toujours en marche » du BT LE, un **développement parallèle a commencé**, au moyen de l'architecture décentralisée proposée par Apple et Google.

- Le **présent rapport est fondé sur l'actuelle version bêta décentralisée de l'application du NHSx**, et non sur le développement parallèle dont les détails n'ont pas encore été dévoilés.

- Les personnes concernées seront des citoyens qui auront installé l'application du NHSx, mais pour le moment, l'application du NHSx **ne traite pas les données sur la base du consentement, mais s'appuie plutôt sur d'autres bases légales**.

- L'**application du NHSx utilise un système de décisions automatisées** (en application de l'article 22 du RGPD), qui n'est pas fondé sur la base légale du consentement. L'application du NHSx ne fait pas appel, de façon importante, à l'IA ou à l'apprentissage machine, mais il est probable que le serveur sonar dorsal le fera (des détails supplémentaires n'ont pas été divulgués).

- Les PECR et la directive relative à la vie privée et aux communications électroniques s'appliqueront probablement aux cookies et technologies similaires, même si cela n'est pas mentionné dans la Trial Privacy Policy. (Le règlement 6 des PECR exige normalement le consentement pour le traitement de cookies ou de technologies similaires, à moins d'une exemption, notamment lorsque le cookie a pour seule finalité d'effectuer la transmission d'une communication sur un réseau de communications électroniques).

- Voir l'encadré 1 ci-après pour les bases légales selon lesquelles l'application du NHSx semble traiter les données.

Bases légales de traitement

SELON LA TRIAL PRIVACY POLICY

La base légale du ministère de la santé et de l'aide sociale (Department for Health and Social Care ou DHSC) pour le traitement de vos données personnelles aux termes du *Règlement général sur la protection des données* (RGPD) et de la *Data Protection Act* (DPA) 2018 est la suivante :

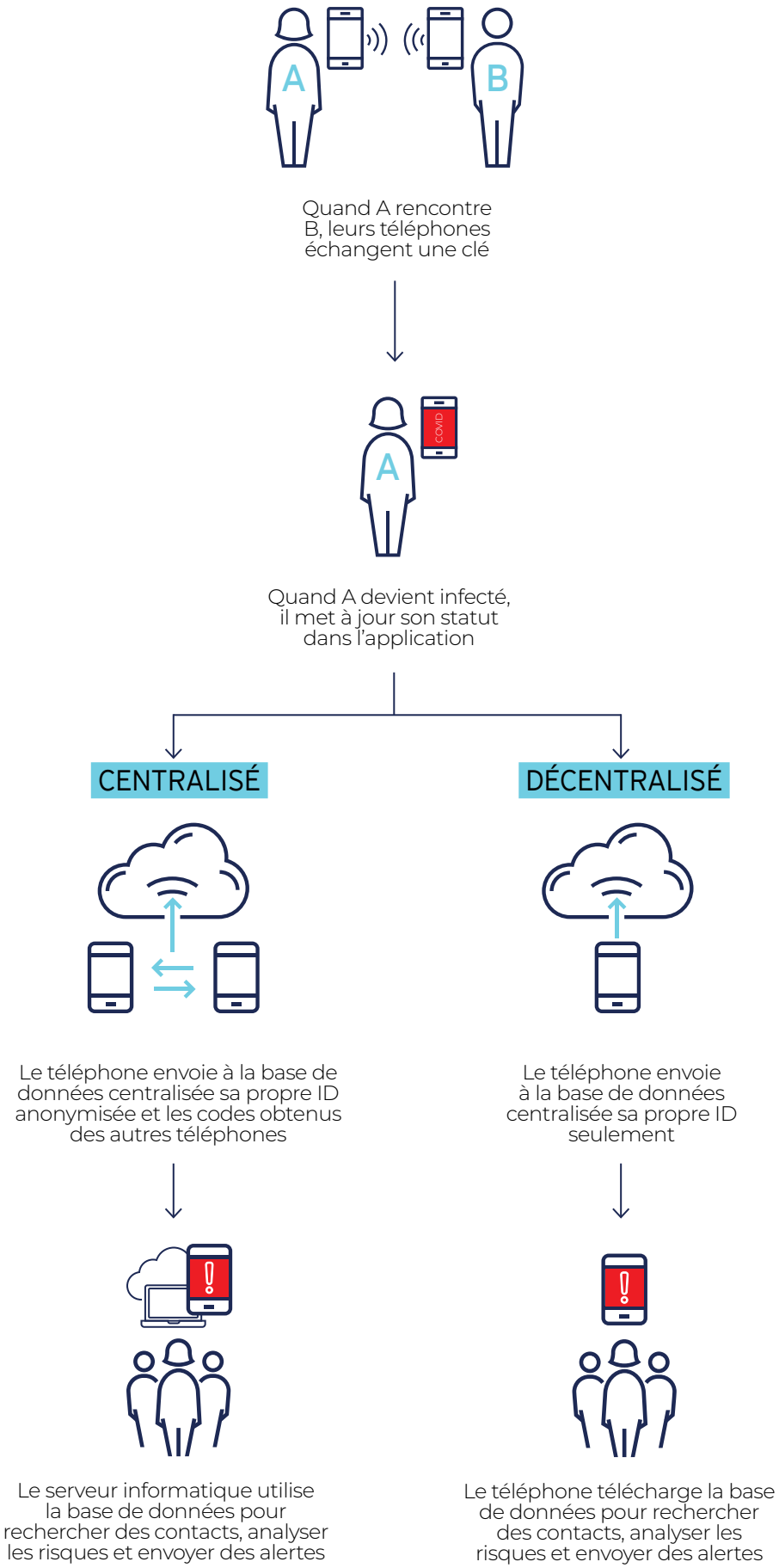
- Article 6(1)(e) du RGPD – le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement*
- Article 9(2)(h) du RGPD – le traitement est nécessaire aux fins de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de soins de santé ou de protection sociale
- Article 9(2)(i) du RGPD – le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique
- DPA 2018 – Schedule 1, Part 1, (2) (2) (f) – à des fins de santé ou d'aide sociale

Les autres organisations impliquées dans le traitement de vos données, comme indiqué dans le présent avis, le feront soit avec un accord en place avec le DHSC pour fournir ce service, soit avec une base juridique qui leur est propre.

L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES DIT ÉGALEMENT :

Exception pour la prestation de services de santé publique conformément au règlement 3 de la *Health Service (Control of Patient Information Regulations) 2002.*

- Bien que l'information communiquée par le système de notification lorsqu'une personne présume elle-même qu'elle est infectée ne contienne aucune donnée sur la santé, **la notification peut éventuellement être considérée comme une donnée sur la santé** ou comme une donnée induite sur la santé, étant donné que seules les données provenant de personnes déclarées positives à la COVID-19 ou présumées comme telles sont téléversées dans le serveur dorsal.
- Le ministère n'a pas suivi la procédure la plus transparente et n'était pas disposé à fournir des informations détaillées sur l'application. Malheureusement, pendant longtemps, de nombreuses informations du domaine public étaient contradictoires et nuisaient à la confiance. **Une analyse d'impact relative à la protection des données a été produite pour l'essai sur l'île de Wight, mais a été publiée après le début de l'essai. Il n'y a pas eu d'analyse en vue d'un déploiement à la grandeur du Royaume-Uni. Nous nous attendons à la publication d'une analyse à court terme.**
- **Il faut un organe indépendant** (comme le recommande le comité conjoint sur les droits de la personne du Parlement britannique) pour superviser l'utilisation, l'efficacité et les mesures de protection de la vie privée de l'application et des données liées au traçage des contacts. L'organe de surveillance indépendant devrait avoir, au minimum, des pouvoirs d'exécution similaires à ceux du commissaire à l'information, pour surveiller le fonctionnement de l'application. Il doit également pouvoir recevoir des plaintes individuelles. L'organe de surveillance doit disposer de ressources suffisantes pour remplir ses fonctions. L'analyse d'impact relative à la protection des données mentionne qu'un **conseil consultatif en matière d'éthique indépendant a été constitué** pour recueillir des avis sur les activités de traitement proposées (bien qu'il ne soit pas clair dans quelle mesure celui-ci peut influer sur la prise de décision du NHSx), et d'autres consultations ont été menées auprès du panel du National Data Guardian et du Centre for Data Ethics and Innovation. **Au minimum, nous recommandons que toute surveillance continue soit assurée par le même groupe d'experts.**
- L'auditabilité doit encore être confirmée, mais le code source sera ouvert et rendu public pour examen.
- L'incidence du **traitement de données par l'application du NHSx est importante** — elle permettra aux citoyens qui ont des téléphones intelligents assez récents de comprendre le risque à savoir s'ils ont été en contact avec d'autres personnes infectées (ou potentiellement infectées) et de les retirer de la chaîne d'infection **en leur proposant, ainsi qu'à ceux avec qui ils vivent**, de s'isoler. En bref, le traitement a une incidence sur la liberté de mouvement et l'autonomie d'une personne (et de ceux avec qui elle vit). L'application du NHSx doit aider le R.-U. (si elle est utilisée avec d'autres mesures) à mieux gérer et atténuer les conséquences des épidémies locales de COVID-19. Ce qui est clair, c'est qu'elle ne peut pas être l'unique solution à la pandémie.


A
B
Quand A rencontre B, leurs téléphones échangent une clé
A
COVID
Quand A devient infecté, il met à jour son statut dans l'application
CENTRALISÉ
DÉCENTRALISÉ
Le téléphone envoie à la base de données centralisée sa propre ID anonymisée et les codes obtenus des autres téléphones
Le téléphone envoie à la base de données centralisée sa propre ID seulement
Le serveur informatique utilise la base de données pour rechercher des contacts, analyser les risques et envoyer des alertes
Le téléphone télécharge la base de données pour rechercher des contacts, analyser les risques et envoyer des alertes

CRITÈRE 1 – BUT ÉTHIQUE ET AVANTAGE POUR LA SOCIÉTÉ

- Contractuellement, l'application du NHSx devra être conforme aux conditions d'utilisation standards de l'App Store d'Apple ou du Play Store de Google, y compris les conditions distinctes relatives à la protection des données personnelles. L'analyse du libellé de ces conditions ne fait pas partie de cette étude, mais ces conditions peuvent avoir une incidence importante sur le traitement des données personnelles par l'application du NHSx. Les fournisseurs de système d'exploitation (Apple et Google) sont avisés que l'utilisateur a installé l'application et s'est inscrit au service de notification poussée, mais ne peut pas voir les données. Toutefois, comme ces fournisseurs offrent le système d'exploitation fonctionnant sur les appareils mobiles, il n'a pas d'autre choix que de leur faire confiance, étant donné qu'ils pourraient éventuellement prendre connaissance d'informations provenant du système de traçage de proximité (comme l'identité de la personne infectée ou de la personne qui en a infecté une autre, ou des graphiques) et qu'il s'agit d'un facteur commun à toutes les applications de traçage des contacts, comme l'application du NHSx.

- Le fait que l'application du NHSx soit une application centralisée et suive un modèle de déploiement gouvernemental illustre bien l'importance de la transparence, l'objectif étant limité, et la collecte et le stockage de données étant réduit au minimum et les données, sécurisées.

- Il apparaît que la réponse des personnes à la notification est volontaire, et qu'un certain degré d'autonomie humaine est préservé. Le message doit moins émotif et moins coercitif que des messages comme « Soutenez notre système national de santé », « Sauvez des vies », « Faites votre devoir de citoyen pour le bien de toute la société », « Faites votre part dans le combat contre le coronavirus ».

- L'objectif initial est louable, mais il existe un risque important de détournement d'usage ou de surveillance de masse, ou les deux. Nous croyons qu'il est primordial de **faire la démonstration de la transparence et de la responsabilité et de faire la preuve que l'application du NHSx est offerte et continue d'être déployée de façon à protéger la confidentialité et d'une manière conforme à l'éthique, tout comme il est primordial de créer un organe de surveillance indépendant**.

- Il existe certains risques associés à ce que pourrait constituer l'application du NHSx pour nous en tant que société et à l'incidence qu'elle pourrait avoir sur nous en tant que société.

  – La promesse d'un avantage pour la santé ou le risque d'une détérioration de la santé chez les personnes atteintes de COVID-19.

  – Nos appareils intelligents pourraient supplanter les êtres humains et les relations avec ceux-ci.

  – Elle a le potentiel de renforcer ou de miner la confiance dans le gouvernement, le système national de santé ou d'autres citoyens.

  – Elle a le potentiel de procurer un faux sentiment de confiance ou de réassurance au moyen d'une solution technologique qui fait partie d'une stratégie plus large.

- Les incidences de tous les autres risques (comme l'identification et la singularisation potentielle des personnes infectées ou des personnes qui doivent s'auto-isoler, ou les deux) et de l'augmentation généralisée du niveau d'anxiété dans le grand public à l'égard du virus et de la peur de quitter la maison ou de circuler parmi la population sont caractéristiques de toutes les autres applications de traçage de contacts et doivent être prudemment soupesées par rapport à l'incidence positive indéniable sur la société (et la santé humaine) de l'utilisation de cette technologie.

- Il semble y avoir un certain flottement au Royaume-Uni quant à l'adoption d'une application centralisée ou décentralisée. L'absence d'ubiquité (c.-à-d. plusieurs applications pourraient être utilisées par la population en général) pourrait réduire l'efficacité de l'ensemble des applications et accroître la confusion au sein de la population. Ce flottement accroît également la complexité des problèmes d'interopérabilité potentiels.

- L'analyse d'impact relative à la protection des données actuelle pour l'essai de l'île de Wight comporte en soi des contradictions quant au traitement des données de l'utilisateur (dans le

contexte de l'application centralisée), ce qui a été fortement critiqué par les militants de la défense de la vie privée et les universitaires. Bien qu'il soit possible que vous puissiez supprimer des données de votre téléphone mobile, il semble que cette suppression n'entraînera pas nécessairement la suppression des données dans le serveur central sonar.

NOTRE RECOMMANDATION

- **L'adoption d'une loi procurant des garanties supplémentaires, y compris des mesures de redressement, comme celles proposées dans le projet de loi intitulé *Coronavirus Safeguards Bill*) contribuera à renforcer la confiance et à atténuer les risques d'échec analysés dans l'EIP.**
- Un plan de protection des exclus du numérique qui n'ont pas accès à un appareil intelligent ou n'en possèdent pas un doit être élaboré, tant pour protéger les exclus (notamment les personnes vieillissantes, les personnes vulnérables, les jeunes enfants, les personnes ayant des besoins de soins de santé ou des problèmes de capacité mentale), mais également à titre de repli stratégique si l'application du NHSx ne fonctionne pas comme prévu. À noter que le NHSx envisage d'adopter l'initiative DevicesDotNow.
- **Il faut s'assurer que des garanties appropriées sont offertes en ce qui a trait aux recommandations et aux notifications et qu'elles sont adaptées et appropriées pour l'utilisateur final** (c.-à-d. que le message doit être adapté selon que le destinataire est un enfant ou un adulte). La vulnérabilité de l'utilisateur déterminera la mesure dans laquelle il se conformera aux recommandations ou pas, et ce qu'il fera de cette information (à noter : risque de suicide ou autres problèmes de santé mentale).
- Les garanties pour tous doivent comprendre **des éclaircissements sur le sort réservé à TOUTES les données une fois que l'application aura été supprimée et sur les circonstances dans lesquelles le système national de santé peut mettre fin au droit d'accès des personnes à l'application du système national de santé**.

CRITÈRE 2 – RESPONSABILITÉ

- Le NHSx est l'autorité de la santé régie par le ministère de la santé et de l'aide sociale (Department of Health and Social Care) du Royaume-Uni. **Il doit être tenu responsable, comme toute autre autorité gouvernementale ou publique**, en particulier en ce qui a trait à la violation des droits de la personne et de la loi sur l'égalité.

- Le système national de santé dont le NHSx fait partie est une autorité de la santé de longue date qui devrait déjà s'être dotée d'une structure organisationnelle et de responsabilité. Cela dit, il n'a aucune expérience du déploiement et de la gouvernance et de la surveillance continues d'outils de traçage de proximité. Bien qu'il ait mis sur pied un conseil consultatif en matière d'éthique, qui offre des conseils au conseil de surveillance de l'application (qui fait vraisemblablement partie du NHSx) (se reporter aux modalités du mandat du conseil consultatif en matière d'éthique), le rôle ou le pouvoir décisionnel du conseil de supervision de l'application n'est pas clairement défini. **Nous recommandons la mise sur pied d'un organe de surveillance indépendant.**

- Il faut établir clairement la nécessité pour le personnel du NHSx de recevoir une formation (le cas échéant) ou pour le NHSx d'en offrir une en interne afin de disposer de la capacité requise en cas de changement de fournisseur de service.

- Il est fort probable que le NHSx, en sa qualité d'autorité de santé publique, et non de fournisseur de solutions technologiques, s'appuiera sur l'expérience de son consortium de fournisseurs de services technologiques, notamment Amazon Web Services (AWS), Pivotal/VMWare Tanzu et Microsoft Azure. L'analyse d'impact relative à la protection des données ou les dossiers de presse ne décrivent pas clairement le rôle (le cas échéant) que joue Palantir au sein de ce consortium, mais peuvent aider à comprendre les données anonymisées. Ces sociétés sont toutes des développeurs expérimentés. **Nous recommandons au NHSx de renforcer sa capacité à cet égard.**

- Fait important (et c'est probablement le résultat de la position de base actuelle adoptée dans l'analyse d'impact relative à la protection des données à l'égard du traitement légal, se reporter à l'encadré 1 qui précède), **les garanties intégrées dans le modèle de l'application du NHSx en matière d'accès et de rectification sont insuffisantes**.

- Les dépendances envers des tiers pourraient également nuire considérablement à la responsabilité à l'égard de la solution. À cet égard, nous devons identifier les principaux fournisseurs de plateforme de système d'exploitation : Apple et Google. **Nous recommandons que ces fournisseurs soient tenus de réaliser des analyses d'impact relatives à la protection des données distinctes et accessibles au public et de fournir un engagement irrévocable ou juridiquement exécutoire en ce qui a trait à la manière dont ils traiteront les données de l'application du système national de santé, y compris les métadonnées sur le comportement des utilisateurs. Ces engagements exigeront non seulement la conformité à aux lois et règlements du Royaume-Uni et aux codes de conduite du NHSx, mais également de la transparence pour permettre de réduire au minimum (et de corriger) les erreurs contenues dans les solutions technologiques de chaque plateforme.**

CRITÈRE 3 – TRANSPARENCE ET EXPLICABILITÉ

- Comme il a été mentionné précédemment, l'application du système national de santé fait l'objet d'un test bêta sur l'île de Wight, un projet pilote visant à évaluer la robustesse du modèle d'application centralisée. Dans le cadre de ce projet pilote, les conditions d'utilisation, une politique de confidentialité et une analyse d'impact relative à la protection des données ont été publiées. Toutefois, les résultats de l'essai réalisé sur l'île de Wight n'ont pas encore été publiés, de sorte qu'aucune conclusion n'a pu être dégagée. Nous attendons également les documents sur la mise en œuvre complète de l'application du NHSx à l'échelle du Royaume-Uni.

- Cela dit, il est possible d'expliquer les fonctionnalités de l'application et les catégories de données utilisées.

- L'application du NHSx est sensible aux risques liés à la technologie Bluetooth LE et à d'autres cyberrisques propres à cette technologie. Ces risques ne sont pas uniques à un outil de traçage

de proximité centralisé, mais sont des risques génériques propres aux solutions décentralisées de cette nature. Nous énumérons certains de ces risques ci-après, dans le contexte du critère 5 (Sécurité et fiabilité) qui suit. Selon nous, la documentation contient peu d'informations permettant de présumer que l'application du NHSx est plus robuste que tout autre système reposant sur la technologie BT LE.

CRITÈRE 4 – ÉQUITÉ ET NON-DISCRIMINATION

- L'analyse d'impact relative à la protection des données pour l'essai réalisé sur l'île de Wight mentionne que l'article 22 du RGPD s'applique, mais que **le consentement ne constitue pas la base sur laquelle ils s'appuient**. Il semble qu'ils s'appuient sur l'exception contenue dans les articles 3(1) et 3(3) du règlement intitulé *Health Service (Control of Patient Information) Regulations 2002* qui « définit les mesures appropriées pour protéger les droits et libertés et les intérêts légitimes des personnes concernées ». Voir **l'analyse juridique de Michael Veale contenue dans l'analyse d'impact relative à la protection des données** qui contient les raisons pour lesquelles cette exception pourrait ne pas s'appliquer à la prise de décisions automatisée.

- En raison de la nature de l'application et du service de notification qu'elle offre, et peu importe que la prise de décisions automatisée s'applique ou non, il est probable que les personnes seront influencées par le biais de confirmation lorsqu'elles accepteront les recommandations de l'application. De plus, il importe de noter que les qualificatifs additionnels suivants pourraient avoir une incidence importante sur l'équité ou la non-discrimination, soit :

  – Le contenu des notifications ;

  – Les sanctions (le cas échéant) en cas de non-conformité à ces notifications (y compris sans s'y limiter des sanctions juridiques, mais également des sanctions liées au retour au travail, en particulier après une période de congé) ;

  – Les limites posées par la conformité ou la non-conformité (p. ex. les contraintes financières ou les circonstances socioéconommiques).

- L'application du NHSx est conçue de manière à ce que la participation se fasse sur une base volontaire. Nous sommes toutefois préoccupés par la possibilité qu'un **segment de la population nationale** (près de 40 % des personnes âgées de plus de 65 ans et de celles âgées de moins de 16 ans) **puisse ne pas pouvoir participer pour la seule raison qu'ils n'ont pas accès à un appareil intelligent ou n'en possèdent pas un**.

- Nous avons déjà indiqué que l'application du NHSx (comme d'autres solutions similaires) pourrait **donner lieu à des comportements de « masse » indésirables dans la société**, ce qui se traduirait par un biais d'automatisation (confiance inconditionnelle dans les résultats fournis par l'application), faussant ainsi la confiance à une extrémité et entraînant l'ostracisation des personnes les unes par rapport aux autres.

- Nous sommes d'avis qu'il **faudrait un système bien établi de redressement** des faux positifs et des faux négatifs, ainsi que des risques de réidentification, des risques de colocalisation et des risques liés aux variables proxy.

- Du fait que l'application du NHSx a recours à un serveur centralisé, il est probable que les **utilisateurs qui se déplacent dans les différents États membres ne pourront pas être notifiés de façon efficace. Il existe un risque important pour les villes frontalières entre l'Irlande du Nord et la République d'Irlande**. Le fait que l'application du NHSx ne soit actuellement pas interopérable avec d'autres solutions de l'UE pourrait être une cause de discrimination ou d'iniquité pour les travailleurs ou les familles interfrontaliers.

- À la lumière de ce qui précède, il existe un risque d'émergence de nouvelles formes de discrimination liées à la possession ou à l'absence de possession de l'application du NHSx.

CRITÈRE 5 – SÉCURITÉ ET FIABILITÉ

- **Tous les systèmes de traçage de proximité qui avisent les utilisateurs qu'ils sont à risque permettent à un adversaire motivé d'identifier la personne infectée** (que ce soit en raison de comptes multiples, d'un enregistrement manuel, de délais d'enregistrement ou d'identification (intervalles de temps), ainsi que d'identification par

photo ou vidéo). Par ailleurs, Il existe des faiblesses inhérentes à la technologie BT LE qui peuvent être exploitées à des degrés divers de sophistication, comme l'injection de bruit, le traçage d'utilisateurs utilisant des projections orthogonales du traçage de contacts (p. ex. adresses MAC), la conduite guerrière et le vol de cellulaires.

- Selon nous, **ces risques dépendent de l'intervention de spécialistes de la technologie et d'acteurs malveillants agissant dans l'intention de nuire**. Comme il a été mentionné au critère 3 qui précède, la documentation contient peu d'informations permettant de présumer que l'application du NHSx est plus robuste que tout autre système reposant sur la technologie BT LE.

- Contractuellement, en ce qui a trait à l'essai réalisé sur l'île de Wight, l'application du NHSx cherchait à atténuer certains des actes de malveillance décrits dans ces conditions d'utilisation au moyen de celles-ci.

- Les points ci-dessus doivent être considérés dans le contexte de l'utilisation de l'application par le grand public. Les niveaux de connaissances technologiques doivent être considérés comme faibles. Les utilisateurs traiteront l'application technologique comme n'importe quelle autre sur leur téléphone. Toutefois, des niveaux de confiance supplémentaires peuvent être présumés, car l'application sera diffusée par le ministère de la santé et de l'aide sociale du Royaume-Uni sous les auspices de l'autorité de la santé, le NHSx. Les attentes en matière de sécurité, de protection contre les risques et de fiabilité de l'application seront donc extrêmement élevées. En outre, il doit être absolument clair que l'application n'est pas un dispositif médical et (malgré les notifications et les recommandations) ne fournit ni ne remplace une assistance médicale. Nous sommes donc préoccupés par le risque de décalage entre les niveaux réels de sécurité et de fiabilité et les attentes du public.

- **Notre recommandation est qu'un programme de sensibilisation et d'éducation du public soit mis en œuvre** d'une manière adaptée au large spectre de la consommation publique. Le Royaume-Uni pourrait vouloir se distancer de la proposition du consortium DP3T de publier une bande dessinée explicative pour faciliter la participation du public.

CRITÈRE 6 – DONNÉES OUVERTES, CONCURRENCE LOYALE ET PROPRIÉTÉ INTELLECTUELLE

- L'application du NHSx en phase de test bêta a été publiée en source ouverte en vertu de la licence du MIT permissive en source ouverte. Compte tenu de ce contexte, nous ne prévoyons pas qu'il y aura des risques complexes liés à la propriété intellectuelle, bien que nous soyons tenus de signaler les modifications découlant des dépendances à l'égard des technologies exclusives, comme le système d'exploitation IOS d'Apple ou Android de Google. Dans une moindre mesure, nous voulons également mentionner que la technologie BT LE est elle aussi une technologie brevetée.

- L'application du NHSx a été conçue pour être utilisée au Royaume-Uni uniquement. Les informations fournies aux fins de l'examen des normes actuelles d'interopérabilité sont insuffisantes, mais, étant donné que l'application repose sur une approche centralisée et n'est pas compatible à l'heure actuelle avec les interfaces de programmation d'applications de Google et d'Apple, il est peu probable qu'elle soit interopérable.

- Comme il est décrit dans l'essai de l'île de Wight :

  – Le partage de données envisagé avec des fournisseurs de services est apparemment assujetti à des contrats conformes au RGPD. L'endroit où sont situés les serveurs en nuage et, par conséquent, où les données sont hébergées n'est pas indiqué clairement (étant donné qu'il est précisé que certains serveurs sont des serveurs d'Europe de l'Ouest ou des serveurs par défaut).

  – Les données seront partagées par NHS England et NHS Improvement en vertu des pouvoirs existants en matière de traitement conformément à l'avis publié par le secrétariat d'État en vertu de l'article 3(4) de la *Health Service (Control of Patient Information) Regulations 2002*.

  – Les données seront obtenues aux fins suivantes : analyse de données pour la planification de la santé publique et la réponse à la pandémie,

comme la planification des ressources et la modélisation épidémiologique, et utilisation de données dépersonnalisées ou anonymisées pour la recherche scientifique et l'analyse statistique.

CRITÈRE 7 - PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

- En général, **nous considérons que les données personnelles peuvent être traitées dans le cadre du système de façon limitée. Il est possible d'utiliser des moyens indirects pour corréler et confirmer des éléments de données personnelles suffisamment pour identifier des personnes**, et ce sera certainement le cas lorsque le consentement aura été obtenu de téléverser des données sur des personnes infectées sur un serveur dorsal. Même si, dans la plupart des cas, la demande dans le cadre de la cause ***Breyer*** auprès de la Cour européenne de justice ne peut être satisfaite, nous sommes entièrement d'accord avec les auteurs de l'analyse d'impact relative à la protection des données qu'une approche conservatrice doit être adoptée et que la solution doit être considérée comme si elle permettait de traiter des données personnelles.

- Nous pensons également que ces données personnelles **pourraient aussi contenir des données potentiellement sensibles (comme des données sur la santé)**. Bien que l'information communiquée par le système de notification lorsqu'une personne se déclare elle-même infectée ne contient aucune donnée sur la santé, la notification peut éventuellement être considérée comme une donnée sur la santé ou comme une donnée induite sur la santé, étant donné que seules les données provenant de personnes déclarées positives à la COVID-19 (ou présumées comme telles) sont téléversées dans le serveur sonar.

- Se reporter au critère 4 et à la rubrique Facteurs justifiant de procéder à une étude d'impact qui précède sur la base légale utilisée pour le traitement des données personnelles dans le cadre du projet pilote.

INRIA and Fraunhofer AISEC ROBERT Protocol PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

15 mai 2020

by Alexander Tribess (Weitnauer Partnerschaft mbB, Germany)
Edoardo Bardelli (Gattai, Minoli, Agostinelli and Partners, Italy)
Licia Garotti (Gattai, Minoli, Agostinelli and Partners, Italy)
Doron Goldstein (Katten Muchin Rosenman LLP, United States)
Dean Harvey (Perkins Coie LLP, United States)
Jenna Karabil (Law Office of Jenna F Karadbil, P.C., United States)
Smriti Parsheera (CyberBRICS Project, India)

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with main PIA for the ROBERT protocol, dated 10 May 2020.

The ROBERT (ROBust and privacy-presERving proximity Tracing) protocol is a proposal for the Pan European Privacy-Preserving Proximity Tracing (PEPP-PT) initiative, whose main goal is to enable the development of contact tracing solutions respectful to the European standards in data protection, privacy and security, within a global response to the pandemic. Therefore, any risks would largely be with the implementing apps. However, many of these risks are inherent with a centralized server system.

It has to be noted that, for the time being, "StopCOVID", supported by the French government, appears to be the only application built on the ROBERT protocol. It has been reported that many other countries that were said to be backing PEPP-PT have now moved to DP3T, using a de-centralized structure instead of the centralized ROBERT approach. Some of the initial developers of the PEPPP-PT are also reported to have abandoned the project due to centralization, transparency and privacy concerns.

The objective of applications such as "StopCOVID" – and the ROBERT protocol behind them – is to trace contacts of a certain proximity and duration between citizens. Once a user gets positively tested on COVID-19, and shares this information with the application (i.e. health data), the application would warn other users that were in close contact with the infected person during the infectious period. To detect whether two users have been in proximity to each other, the applications rely on short-range communications exchanged using the Bluetooth wireless technology activated on both users' devices. Thus, the application could help facilitate and accelerate the spread of information amongst citizens concerning possible infections.

One of the ideas behind the PEPP-PT initiative was to develop a protocol that could serve as a basis for various "national" apps which would then be able to interact with each other. Especially within the European single-market and the Schengen area, cross-border travel is likely to increase significantly once travel restrictions have been withdrawn. Therefore, it is likely that applications based on the ROBERT protocol will be used for cross-border travel and, thus, in different jurisdictions.

As applications based on the ROBERT protocol would be processing personal data of users, the main regulatory requirements would be laws on privacy and data protection (such as the GDPR for EU/EEA member states, or national laws on data protection, e.g. in Switzerland). The main ethical concerns are that (a) a centralised system could be more amenable to mission creep by the governments ; (b) people could be stigmatized if, by using the application, it would become publicly known that they had been infected with COVID-19 and spread the disease ; (c) from the data collected through the application, malicious users and/or organizations could draw contact and/or movement profiles of a large number of people.

As regards the stakeholders, apart from the developers of ROBERT itself, a couple of other

stakeholders need to be considered: There will be developers of the applications based on the ROBERT protocol. It is likely that applications would be provided by government agencies (e.g. national health agencies) ; however private initiatives are not excluded from using the protocol. As the ROBERT protocol suggests a centralized model, there must be a provider for the central server (perhaps a national health agency if run by a government).

The ROBERT developers team puts a strong emphasis on the fact that data would be transmitted pseudonymously. In addition, due to the centralized server model, the protocol does only collect very little information on the concrete circumstances of a contact. With a centralized approach, the calculation of the risk of contagion is done on the server side, without taking into account the quality of contacts nor personal information. The result could, therefore, be unreliable, with probably many false positives as opposed to a de-centralized approach where much more information may be collected and stored on the user's device. In terms of explainability, the results (i.e. the warning messages sent to users) cannot be explained to the specific user because the user will not get any information on the location or exact time of the contact ; the user must trust the application without being able to gather any further information as regards the "real" risks.

Data will be processed on a very large scale. It is the idea behind any contact tracing solutions that as many people as possible have respective applications on their mobile devices and keep them activated. If applications were actually used by a very large number of people in a given populations (maybe 60 % or more), contact tracing applications are said to become an important instrument to contain the virus.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

ROBERT could provide the deployer – being it national or private (i.e. a research institute) – with a better understanding of the spreading of the pandemic and – potentially – it may contribute in flattening the epidemiological curve.

However, the technology itself, and especially the risks that are inherent to the centralized structure, also bear the risk that data collected through applications could be processed for other purposes than mitigating the COVID-19 pandemic by tracing contacts. The more contact information is transmitted to the server, even if this information is pseudonymized/anonymized, the greater the risk of attacks. The more information the central server stores, the greater the risk of loss of anonymity and confidentiality, as the success of cryptanalysis attacks increases with the amounts of encrypted samples available.

It must be noted, also from an ethical perspective, that the ROBERT protocol is published under an OpenSource software license (MPL 2.0, https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux). Thus, it may well be that the technology is used in parts of the world that do not follow strict legal principles, including the declarations of human and citizen rights, laws on privacy, data protection, non-discrimination, etc. These risks are imminent considering that there have just recently been serious impairments concerning the rule-of-law principle even in some EU member states (such as Poland and Hungary).

Notwithstanding the aforesaid, any implementation of the ROBERT protocol under a given jurisdiction, and even the selection of the app supporting device (app, mobile device, wearable, etc.) may entail other legal, cross border, policy, or contractual obligations that have not been subject to this PIA.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, there may be other risks to consider that come along with third-party dependencies of the applications. These will depend on the security model e.g. of the mobile operating system, which may have access to all data stored in the application provided that such access is allowed by the applicable laws.

Bluetooth is used for contract tracing in ROBERT by using the beacons principle – that is, devices signal each other with short information, without the need to establish a Bluetooth connection between them. Messages are sent to all devices with Bluetooth enabled, there is no ability to send a message to only certain, authorized devices. Thus, it is easy for anyone to listen to everything that happens on the Bluetooth signal. For these reasons, it is possible to spread malicious information. This risk becomes even more crucial considering that the applications

need to be continuously running, with Bluetooth connections activated. Moreover, in order to prevent "one entry" attacks, the server may introduce some randomly selected false positive. In light of the above, accuracy might be at risk and, consequently, it might generate negative consequence where such are not needed (i.e. self-isolation where the contact is not positive). It is noted that several improvements have been made to the ROBERT protocol in an attempt to mitigate or prevent such risks. However, it is impossible to eliminate the risks inherent in using a protocol based on Bluetooth.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

Users have an interest in understanding the risk of intrusive surveillance, long term tracking and the potential for identifying infected individuals, and in the risk scoring algorithm of any particular implementation.

It is possible that the app implementer could also choose to use the algorithm for purposes such as to determine priority of testing or confinement decisions which could have a significant impact on the rights of users.

When a user's positive status is communicated to the central authority it will assign an "at risk" status to the persons who are shown to have come in contact with the positive case. Due to limitations intrinsic to the Bluetooth technology, proximity tracing solutions may lead to false positive and/or negative (see above). The determination of the risk status is therefore subject to the accuracy limitations of Bluetooth technology. In addition to proximity information, risk scores maybe based on other parameters to be decided by the implementor, in collaboration with epidemiologists. The developers of the protocol note that the actual effect of the false positives will depend on the purpose for which the app is being used. They note that a false positive is more problematic if the fact is to notify the user to go into quarantine as opposed to a case where the user is only advised that he or she should get tested.

ROBERT does not require disclosure of adoption rates. It is the idea behind any contact tracing solutions that as many people as possible have respective applications on their mobile devices and keep them activated. Without information available on adoption rates, the efficiency of the Pandemic Tech Solution may be at risk.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

ROBERT is not an application but a communication protocol. One of its design goals is that participants should be able to join or leave the system at any point. The final decision on whether to make the application voluntary or compulsory will be made by the organisations that adopt the protocol. The French Government's present position is that the StopCovid app will be available on a voluntary basis. A final determination is not possible at this stage as the app has not yet been launched.

The requirement of Bluetooth enabled smartphones as the basis of the protocol limits the participation to persons who have access to such devices. In particular, children who do not have their own devices and others such as the elderly and persons with disability who might have trouble engaging with the app could be excluded from the contact tracing mechanism. Accordingly, any conclusions about the aggregate risk profile based on statistics collected from the app may not reflect the cases of persons belonging to these groups.

Depending on the implementation of the ROBERT protocol, false positive results may be of discriminatory effect (see above).

Adherence with the standards and guidelines of the World Wide Web Consortium's Web Accessibility Initiative can help in reducing accessibility barriers in the design and implementation of the solution.

PRINCIPLE 5 – SAFETY AND RELIABILITY

The centralized server structure is the weak point in the ROBERT protocol. Risks of using such centralized system include the following:

Single point of attack: Any breach in a server would endanger the whole federated system and all users of affected applications. Intruding the server could result in the identification of users.

Linkability of users: With a centralized system, the server is able to learn and potentially piece together information about specific users. The server could infer that two infected users were in contact at some point in time based on timestamps, allowing the server to build a partial social graph that reflects these encounters. Furthermore, the server could identify anonymous uploaders with co-locations by performing a frequency analysis on the uploads and cross referencing with who performed the uploads. In addition, the server could identify anonymous uploaders with causality, as causality is preserved in the uploads. Thus, the server can reconstruct a pseudonymous graph using time causality.

Tracing of users: The centralized server creates ephemeral identifiers and can, at any point, link the past and future ephemeral identifiers of any user, infected or not, by decrypting back to their permanent identifier. In combination with other data sets, such as CCTVs, the server can therefore track all individuals, infected or not. Given a target ephemeral ID, such as one collected by law enforcement from a suspect, it is possible to tag and classify individuals that third parties can recognize without access to the centralized server or database. ROBERT's ephemeral IDs are not authenticated, and the server does not provide any proof that they are an encryption of the ID, or that the correct key was used. This capability could allow law enforcement, or other actors, without any access to the backend database, to track the movements of specific users and communities by assigning them distinguishable identifiers and recognizing their tagged Bluetooth emissions. This could enable long-term tracking of individuals or communities (as one could assign specific identifiers to target groups of people) by third parties. Moreover, users could also detect others EBIDs and use them maliciously.

A contact tracing application based on the ROBERT protocol must be widely used and run efficiently to meet the goal of aiding in the containment of the COVID-19 pandemic. However, some characteristics of the present ROBERT protocol give rise to concerns as regards the efficiency of such applications. A technical failure of ROBERT would mean that a user is potentially either not able to share their infected status and thus help notify other users or does not receive notification about having been in proximity to an infected person when queried. In both cases, users may have been exposed, but they will not be notified and thus could be further exposing others by not taking protective measures.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

IP ownership in implementations of the protocol will depend on the choices made by the implementers. Licensing terms of particular implementations (open source or otherwise) will be determined by the implementers.

Under the protocol, data are captured and stored by unique ID/user and EBIDs and by timestamps. The protocol requires sharing of unique IDs/EBIDs in order to map potential infection vectors. The protocol describes NATs (Network Address Translation) as potential mitigation for individual uploads, but notes the limits of NATs both in terms of prevalence and location grouping. The protocol also notes that to ensure network-layer unlinkability, the actual application implementations must be unlinkable using anonymous authentication mechanisms and rate-limiting mechanisms to upload large numbers of observations

PRINCIPLE 7 – PRIVACY

Though many of the above-described risks already could have adverse effects on user's privacy, there are some further privacy concerns that come with the ROBERT protocol.

As outlined before, ROBERT is a protocol, thus a technical basis on which various applications may be deployed. Therefore, any risks would largely be with the implementing apps. However, many of these risks are inherent with a centralized server system. As any application based on the ROBERT protocol would be processing personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), these risks are even more considerable.

Data are stored in the server for three weeks. However, this should be balanced with public health necessities and, in particular, with the pandemic's incubation period. If data retention periods are not minimized, the application based on the ROBERT protocol may infringe the principles of necessity, proportionality and data minimization.

Providing exhaustive and transparent information on the processing of personal data may, under certain jurisdictions or laws (such as the GDPR), be a mandatory legal requirement to observe. However, from the information available on the ROBERT protocol itself, not all mandatory information can be retrieved.

CONCLUSION

The ROBERT protocol with its centralized server structure brings a lot of inherent risks as regards user privacy and data security. Whereas other concerns (such as, for example, regarding non-discrimination, fairness, efficiency) may relatively easy be mitigated by implementing privacy-by-design principles into the applications, the architecture of the protocol itself remains critical. ROBERT may be used for purposes that go way beyond what is necessary in order to mitigate COVID-19, and it may turn out, depending on the organization deploying the application, to become an instrument of mass surveillance.

Although, certainly, also a de-centralized server structure does not come without privacy risks (comp. Serge Vaudenay, Analysis of DP3T – Between Scylla and Charybdis, Lausanne, 8 April 2020, https://eprint.iacr.org/2020/399.pdf), at least the risk of being silently converted into such an instrument of mass surveillance must be considered much lower when using a de-centralized system architecture.

Robert-Koch-Institut (RKI)
Corona-Datenspende PostCoviData
Impact Assessment (“PIA”)
Overarching Risk Summary (Key Findings)

12 mai 2020

by Alexander Tribess (Weitnauer Partnerschaft mbB, Germany)

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with main PIA for Corona Datenspende, dated 11 May 2020.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

On 7 April 2020, the Robert-Koch-Institut (RKI), the German federal agency for public health, published a corona data donation app for Android and iOS. The RKI app is designed to make users donate to the agency health data from their wearables/fitness bracelets/fitness apps. The RKI aims to derive from such data information on the spread of COVID-19 nationwide and on a regional level.

The goal of the “Corona-Datenspende” (corona data donation) app is to improve prediction possibilities for the nationwide spread of COVID-19 based on unspecific health data (such as pulse rates) and, thereby, to accelerate and focus future containment measures in identified high-risk areas. That being said, the focus of the project is to serve public health as opposed to give the donating user an indication as to whether he or she may be infected.

Considering that testing capacities are limited and, even more importantly, many COVID-19 infections come with only very mild symptoms (so that infected people are unlikely to ever ask for a test themselves, but may, however, spread the virus to others that develop a more severe illness), the RKI aims to better estimate the possible number of undetected COVID-19 infections. The project has been publicly supported by the German Federal Government and, especially, by the Federal Ministry for Health.

Germany can be considered one of the best developed democracies of the world, with a high standard in terms of implementing rule of law. Processing of personal data in Germany (being a member state of the EU) is subject to the GDPR, also for government agencies. In addition, for eGoverment applications, the *Bundesamt für Sicherheit in der Informationstechnologie* (BSI, German federal agency for security in information technology) has published directive BSI TR-03107-1 in 2019, which also apply to the Corona-Datenspende application.

The RKI has been working on this project together with a developing partner from the private sector ; examination of the data derived from the use of the app will be conducted in collaboration with two German universities (Humboldt Universität Berlin, FAU Erlangen-Nürnberg).

The main ethical concerns are that (a) from the data collected through the application, malicious users and/or organizations could get personal health information from a large number of people, (b) malicious users could, by falsifying information uploaded to the RKI, influence and interfere with the containment measures. It is to be noted in this context that the RKI is a direct advisor to the federal government, and its advice is also considered by any other state or private decision-makers ; influencing the data could, thus, have direct effects on public and private pandemic mitigation measures.

Though the individuals directly affected by data processing through the app are limited to users of wearables and other fitness tracking applications (such as iOS Health) voluntarily donating their data to the RKI, the impact of the app on the general public must not be underestimated. The "Corona-Datenspende" app has been developed and published very quickly upon the detection of the first COVID-19 infections in Germany. It has now been available for more than a month and has found a significant number of users (about 500,000).

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The app being provided by the German federal agency for public health and publicly promoted by the government, its impact on future government measurements to mitigate the COVID-19 pandemic and, thus, its societal and economical effects cannot be underestimated.

Successful attacks on the information security or widespread malicious use of this app have the potential not only to weaken the acceptance of and trust in any app-based measures to contain the pandemic, but they may also cause severe harm to societal and economic welfare in Germany and, considering Germany's importance for the European single market and in international trade, also abroad. Thus, any risks as regards the security of the app create a significant risk to society as a whole, perhaps even on a global level. In addition, any shortcomings in the protection of collected data as well as erroneous forecasts and measures could have a significant impact on the public perception of the RKI itself.

The laws and the legal system in Germany, in general, may be considered sufficient as to mitigate the risks associated to the application. The German federal commissioner for data protection and freedom of information (BfDI) will supervise the deployment and use of this app.

On an individual level, users are free to install and install the app. Depending on the devices they use, they are able to decide which data to share and which to withhold. Users can prevent the app at any time from processing data by switching off or not wearing their wearable. The most important risk for users would be if their share of the data collected by the RKI could be associated with a specific user, i.e. if they were re-identified.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, it has to be noted that the RKI app is fully dependent on third-party devices or apps. These come with certain risks themselves, the gravity of which will depend on the security model e.g. of the mobile operating system.

The app provider is a software enterprise that has been dealing with eHealth projects in the past. It could have been expected that this provider was capable of implementing mandatory GDPR principles such as, for instance, Privacy be design (Art 25 of the GDPR).

The principles of necessity, proportionality and data minimization allegedly have been observed. However, as it remains unclear which data are being processed exactly and for which particular purposes, it cannot be ascertained whether all data are actually required for these purposes. The lack of explainability certainly constitutes a problem ; however, data are said to be transmitted only pseudonymously and anonymized before further processing. It is somewhat typical to scientific processing, that the purposes and the scope of such processing may evolve over time.

Development and deployment are publicly funded. Therefore, if it turned out that mitigating some of the risks identified herein, would come with additional costs, it is very likely that the RKI would decide to spend more rather than accept both avoidable and inacceptable risks.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

As noted above, decisions of the RKI based upon the data derived from the "Corona-Datenspende" may have a huge impact on society. However, the RKI server offers easy ways to create fake pseudonyms with a freely selectable postal code. In addition, knowing the pseudonym of a data donor, third parties can retrieve his authentication token from the RKI server and thus send further data to the RKI under the pseudonym of the data donor, including, for example, the number of steps taken or other activity data. Third parties can also connect their own

fitness tracker and thus their health data with the pseudonym of another user. These risks must not be considered only theoretical because they do not require high-level technical skills. That being said, there is a significant risk (especially in regions with only a small number of users) that data collected through the app may be faulty. This could lead to false predictions in either direction. In terms of transparency, the public most likely cannot and will not be informed about rates of false data input at all.

Though it must never be forgotten that the app is not supposed to serve the individual benefits of its users but the general public, it remains questionable that the RKI provides so little information on the specifics of (algorithmic) data processing operations and the processes of risk analysis. For instance, from the information available so far, users would know that they are to provide their postal code (whereby only the first two digits will be further processed). Furthermore, users know that any analysis from the RKI on the basis of their data will be made on "Landkreis" level. However, this is irritating and requires further explanation as German postal codes are not in any way associated with the "Landkreis" regions (comp. fig. 1 and 2 below, both published in the public domain under CC0 1.0 license). Thus, it remains completely unexplained how the RKI could be able to detect infection risks on a "Landkreis" level on the basis of the first two digits of a postal code. (please note: German postal codes consist of five digits, the first two of which indicate a region of the country that is usually significantly bigger than a "Landkreis", however, big cities are divided into numerous regions, like for instance Hamburg using 20xxx, 21xxx, 22xxx postal codes).

German "Landkreise" (*fig. 1 left*) and German postal code areas (*fig. 2 right*). It can be seen from the maps that sometimes more than one "Landkreis" is covered by a postal code area, whereas in other cases (especially in big cities) one "Landkreis" belongs to numerous postal code areas.
In terms of explainability, it remains entirely unclear how the RKI is supposed to draw conclusions for a "Landkreis" from information based on the first two digits of postal codes.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The data are collected from an undefined and unrefined group of users. The datasets (especially data on activity levels and data concerning health like pulse rates etc.) cannot be biased themselves. Data are donated by users on a voluntary basis.

Users would never be directly affected by individual decisions of the app or based on the data derived from the app. It would only be possible that, based on information collected through the app, the RKI provides advice to government officials that would then perhaps initiate or lift certain containment measures. Thus, if data input was false or corrupted, individuals, as part of the society, could be treated "unfair".

PRINCIPLE 5 – SAFETY AND RELIABILITY

Technical analysis of the RKI app revealed a variety of major security risks associated with the setup of both the server and the data transfer mechanisms. This revelation is even more concerning as, also considering the communication from the RKI, users are to expect a maximum of data security. As the RKI app processes personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), these risks are even more considerable. The entire model of donating one's personal data for the purposes of serving public health depends on users' trust. Thus, severe shortcomings in data security may endanger the project as a whole.

Any breach in a server would endanger the whole federated system and all users of "Corona-Datenspende". Intruding the server could result in the identification of users. Analysis has revealed obvious shortcomings in server security, though.

The actual data transfer mechanisms for third-party devices and Google Fit are inconsistent with public communications of the RKI. The RKI server gets direct access to and received the data stored on the servers of the fitness tracker provider or data stored at Google Fit. Access data allow access to non-pseudonymized and historical fitness data and, in the case of the providers Fitbit, Garmin, Polar and Google Fit, access to the full names of the data donors, Direct access of the RKI to the fitness data is not even automatically terminated when the smartphone app is uninstalled.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The app is clearly not designed for data sharing purposes other than with the RKI itself. The data collected through the app will remain with the RKI and its research partners. Data collected through the app are being used for further scientific research on the field of public health.

RKI is mentioned as copyright holder in the iOS app store ; parts of the copyright to the solution, under German copyright law, necessarily remain with the actual developers. That being said, it seems unlikely that the app is going to be distributed to other pubic health agencies in the world.

PRINCIPLE 7 – PRIVACY

Though many of the above-described risks already could have adverse effects on user's privacy, there are some further privacy concerns that come with the "Corona-Datenspende" app.

Consent is implemented by an opt-in procedure (i.e. activating a checkbox underneath the privacy notice). This means that consent shall be declared electronically using non-signature-based processes. However, this is not in line with government agency directives binding on the RKI. Apart from these directives, there have been several Court decisions indicating that consent under the GDPR may solely be valid if the identity of the data subject is undoubtedly clear. Thus, the RKI's approach not to check on user's names in order to keep their identity pseudonymous, may lead to an infringement of data protection principles in itself (Art. 9 para. 2 of the GDPR).

The age limit of the app is set to "4+" at least in the iOS app store, which indicates that the app was designed for use also by small children. During the registration procedure, the user must confirm that he or she was at least 16 years of age. However, this does not constitute an age verification mechanism worth mentioning. Considering that, under Art. 8 of the GDPR, where consent is required in relation to the offer of information society services directly to a

child, the processing of the personal data of a child shall only be lawful where the child is at least 16 years old, this constitutes a crucial weakness.

As the RKI does not actually know its users (see above), there are further shortcomings in terms of mandatory data protection obligations. Any data subject has the right to access information being processed about him or her (Art. 15 of the GDPR) ; data subjects may also request correction or deletion of their data under certain circumstances (Art. 16, 17 of the GDPR). However, any such right may only be granted to a person that can clearly considered to be the actual data subject. Providing access to a data subject's personal data to a person other than the data subject itself would constitute a severe breach of GDPR obligations. Considering that the RKI does not know its users, the only way for the RKI to deal with possible data subjects' requests would be on the basis of the pseudonymous codes being provided to the users during the registration procedures. However, as has been shown, these IDs are neither secret nor protected against unauthorized copying.

The actual data processing operations through the RKI app differ from those stated in the Privacy Policy. Whereas, in the Privacy Policy, the RKI states that (a) data were pseudonymized on the device, (b) no direct identifiers such as names were submitted to the RKI, and (c) data were transferred solely via the user's smartphone, CCC analysis has revealed that quite the opposite is true.

CONCLUSION

The RKI app has the potential of improving the predictability of the spread of COVID-19. However, considering the key role of the RKI within the German response to the pandemic, the data basis for RKI predictions must adhere to the highest standards of reliability. As CCC analysis has revealed, the app itself, its connection to third-party providers, such as health apps and wearables/fitness trackers, and its server infrastructure show some significant shortcomings in terms of data security. At least some of these flaws could have been easily avoided, and it raises some concern that RKI's partners did not implement appropriate safeguards in the first place. Even though some of the deficiencies may have already been cured and others certainly can be rectified, there is a remainder of risks that adversely affect the fundamental human right to privacy as well as the overall reliability and efficiency of the entire app.

In the current state, the "Corona-Datenspende" app must be considered an infringement and the RKI to be in breach of mandatory GDPR obligations, including, without limitation, the principles of data minimization (Art. 5 para. 1 lit. c of the GDPR) as well as integrity and confidentiality (Art. 5 para. 1 lit. f of the GDPR), the accountability obligations of the controller (Art. 5 para. 2 of the GDPR), the lawfulness of processing personal data (Art. 6, 8, 9 of the GDPR), the data subjects' rights (Art. 15 et seq. of the GDPR), the general responsibilities of a data controller (Art. 24 of the GDPR), the core principle of data protection by design (Art. 25 para. 1 of the GDPR), and the obligation to implement adequate technical and organizational measurements to ensure an appropriate level of security (Art. 32 of the GDPR).

Apple/Google Contact Tracing Exposure Notification API Apple/Google API PostCoviData Impact Assessment ("PIA")

June 3, 2020

ItechLaw Evaluation Committee
Charles Morgan, McCarthy Tétrault LLP
Pádraig Walsh, Tanner De Witt Solicitors

© ItechLaw Association 2020, CC-BY-SA

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- "**Apple/Google Contact Tracing API**", in short "**Apple/Google API**", is a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing.

- Google and Apple announced a two-phase exposure notification solution that uses Bluetooth technology on mobile devices to aid in contact tracing efforts.

- According to the Apple/Google API Exposure Notification FAQ (https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf):

  – Both phases of the solution harness the power of Bluetooth technology to aid in exposure notification. Once enabled, users' devices will regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier — basically, a string of random numbers that aren't tied to a user's identity and change every 10-20 minutes for additional protection. Other phones will be listening for these beacons and broadcasting theirs as well. When each phone receives another beacon, it will record and securely store that beacon on the device.

  – At least once per day, the system will download a list of the keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19. Each device will check the list of beacons it has recorded against the list downloaded from the server. If there is a match between the beacons stored on the device and the positive diagnosis list, the user may be notified and advised on steps to take next.

  – To power this solution in the first phase, both companies will release application programming interfaces (APIs) that allow contact tracing apps from public health authorities to work across Android and iOS devices, while maintaining user privacy. These apps from public health authorities will be available for users to download via their respective app stores. Once the app is launched, the user will then need to consent to the terms and conditions before the program is active. The companies plan to make these APIs available in May.

  – In the second phase, available in the coming months, this capability will be introduced at the operating system level to help ensure broad adoption, which is vital to the success of contact tracing. After the operating system update is installed and the user has opted in, the system will send out and listen for the Bluetooth beacons as in the first phase, but without requiring an app to be installed. If a match is detected the user will be notified, and if the user has not already downloaded an official public health authority app they will be prompted to download an official app and advised on next steps. Only public health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control.

  – If at some point a user is positively diagnosed with COVID-19, he or she can work with the health authority to report that diagnosis within

the app, and with their consent their beacons will then added to the positive diagnosis list. User identity will not be shared with other users, Apple and Google as part of this process.

- According to the Apple/Google API FAQ, if a user decides to participate, exposure notification data will be stored and processed on device. Other than the random Bluetooth identifiers that are broadcast, no data will be shared by the system with public health authority apps unless one of the following two scenarios takes place:
  - If a user chooses to report a positive diagnosis of COVID-19 to their contact tracing app, the user's most recent keys to their Bluetooth beacons will be added to the positive diagnosis list shared by the public health authority so that other users who came in contact with those beacons can be alerted.
  - If a user is notified through their app that they have come into contact with an individual who is positive for COVID-19 then the system will share the day the contact occurred, how long it lasted and the Bluetooth signal strength of that contact. Any other information about the contact will not be shared.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Generally, use of the app is intended to help flatten the epidemiological curve of local COVID-19 epidemics and avoid new outbreaks by assisting with contact tracing, while protecting individual privacy.
- Given the emphasis placed on user opt in and voluntary self-notification, and the primacy of human right to health and life, Apple/Google API achieves a balance between rights of the individual and rights of the community.
- In particular, it is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information regarding with respect to other users.
- As we currently understand it, there are no forced auto installs proposed of Apple/Google API, but this will depend on functionality implemented at national levels.
- Subject to national implementations adding functionality, there are currently no automated decision making implications
- The general overarching risk of this app is that (like any other proximity/contact tracing application) it could be used for other purposes post-pandemic.
- We consider that the wider risks of repurposing this app for other state sponsored uses have been adequately mitigated by its distributed architecture. Google and Apple have indicated that they will disable the exposure notification system on a regional basis when it is no longer needed.
- Any other risks (such as for example, the identification and potential singling out of infected individuals and/or those that are required to self-isolate) would be generic to all other contact tracing apps and need to be balanced carefully against the undoubted positive impact to society (and human health) in the use of such technology.

PRINCIPLE 2 – ACCOUNTABILITY

- The API is provided by Apple and Google who will be accountable upon failure. Accountability is also likely to reside with the national health authority adopting Apple/Google API architecture for local/national implementation – ie. ultimately the national government."
- Apple and Google are project sponsors and providers of the API. The front-end apps will be developed by local government or public health agencies
- We have not seen details related to the governance structure for this offering

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- As the Apple/Google API system depends on conventional BT LE technology for proximity tracing, the system demonstrates equivalent levels of robustness which would be exhibited by any other distributed network/system.
- The Backend and Authorisation servers should be fully auditable, subject to access being provided by local implementing authorities. We observe that this is not a centralised system – it is highly

distributed. Local data held on smartphones will be outside scope of inspection and audit unless access is granted by (or court orders are sought effecting same).

- Both Google and Apple have published a joint suite of documents aimed at explaining technological features of the API – see apple.com/covid19/contacttracing/ These specifications comprise (i) BT Specification (ii) Cryptography Specification and (iii) Framework API document outlining on a technological basis how they will implement such apps in their OS.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- The choice to use this technology rests with the user, and he or she can turn it off at any time by uninstalling the contact tracing application or turning off exposure notification in Settings.

- There will be no monetization from this project by Apple or Google.

PRINCIPLE 5 – SAFETY & RELIABILITY

- As the Apple/Google API system depends on conventional Bluetooth Low Energy technology for proximity tracing.

- Bluetooth Low Energy has inherent weaknesses which are capable of exploitation with varying degrees of sophistication, such as noise injection, tracking of users using aspects orthogonal to contact tracing (ie. by logging MAC addresses), wardriving, and theft of mobile phones.

- The system demonstrates equivalent levels of robustness which would be exhibited by any other distributed network/system

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to interoperate internationally.

- Apple/Google have authored an open source reference implementation of an Exposure Notifications server: https://github.com/google/exposure-notifications-server

PRINCIPLE 7 - PRIVACY

- Contractually, Apple/Google API will require to conform to both Apple's App Store standard agreement and Google's Play Store Agreement. Each of these agreements contain separate privacy related terms (Google Play store for example refers to Google's Privacy Policy, see section 9 of that Agreement ; also see section 5.1 Apple's App Store Developer Agreement).

- According to Google and Apple, they have put user privacy at the forefront of this exposure notification technology's design and have established strict guidelines to ensure that privacy is safeguarded:

  – Consistent with well-established privacy principles, both companies are minimizing data used by the system and relying on users' devices to process information.

  – Each user will have to make an explicit choice to turn on the technology. It can also be turned off by the user at any time.

  – This system does not collect location data from your device, and does not share the identities of other users to each other, Google or Apple. The user controls all data they want to share, and the decision to share it.

  – Random Bluetooth identifiers rotate every 10-20 minutes, to help prevent tracking.

  – Exposure notification is only done on device and under the user's control. In addition people who test positive are not identified by the system to other users, or to Apple or Google.

  – The system is only used for contact tracing by public health authorities apps.

  – Google and Apple will disable the exposure notification system on a regional basis when it is no longer needed.

TraceTogether Bluetooth-based contact tracing system PostCoviData Impact Assessment ("PIA") – Key Findings

May 20, 2020

ItechLaw Evaluation Committee
Pádraig Walsh, Tanner de Witt
Philip Catania, Corrs Chambers Westgarth

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with draft PIA and whitepaper for BlueTrace protocol.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- "**TraceTogether**", is a Bluetooth-based application running on the BlueTrace protocol with the aim of assisting and increasing the effectiveness and efficiency of contact tracing. TraceTogether was launched in March 2020 and is downloadable through the Apple AppStore and Google Play.

- TraceTogether will record who a user has been in contact with, but not where. The devices that are running the TraceTogether application will actively communicate with nearby devices and will only record information regarding the proximity of the other device and the duration of the contact.

- Users of TraceTogether are only required to register their phone number with the application. No other personal information is obtained. Upon registration, the user will be issued with a user ID ("**UserID**") for identification purposes.

- A TempID ("**TempID**") is generated by the back-end server to the device on a temporary basis. The TempID is mainly used for communication between devices and only the Ministry of Health of the Republic of Singapore ("**MOH**") has the secret key to decrypt the TempIDs to reveal the underlying UserID, created time and expiry time. The temporary ID is random, anonymized and refreshed at regular intervals.

- Upon a user being diagnosed with COVID-19, the MOH seeks the user's consent to share the stored encounter information to the back-end server (being the TempIDs the user's device has retrieved and stored). The MOH seeks personal confirmation on the physical encounters that the user can remember. The MOH will decrypt the information and analyze the encounters to determine whether they need to be in touch with any other users who have been in close encounter with the COVID-19 contracting user.

- The goal of this project is to assist public health authorities in their efforts to fight the spread of COVID-19 by notifying users of at-risk interactions with patient users allowing potential patients of COVID-19 to be identified in a privacy-preserving manner.

- TraceTogether is designed so that only the MOH will have access to the phone numbers of the users, subject to the user consenting to the sharing of the information. The information collected by the MOH (and on the device) will only be used for COVID-19 contact tracing. It also appears that the MOH is committed to safeguarding the information collected and will not disclose the data to any other users.

- TraceTogether will only collect data on the basis of consent ; the installation of TraceTogether is voluntary.

- The information collected through TraceTogether will not be used to make decisions about the individuals ; rather it will be used (anonymously) to supplement the existing contact tracing practice as adopted by the MOH. It is not intended that TraceTogether will replace the existing manual practice.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Generally, use of the app is intended to help control the widespread of COVID-19 and to take patients into treatment at an early stage by assisting with contact tracing, while protecting individual privacy.

- It is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on identifying Encounter Information of COVID-19 diagnosed patients to contact other users who may had been in close contact with such diagnosed patient.

- TraceTogether is designed to promote human agency and autonomy

  – Users will have opportunities to provide express consent on downloading the application, allowing the application to send and record Encounter Messages and on sharing such Encounter Messages to MOH.

  – TraceTogether does not process any information collected through the application, it is not designed to operate with AI/ML.

  – TraceTogether does not use any data to diagnose potential patents of COVID-19, instead it merely collects information of whether any other users had been in close contact with the diagnosed patient in order for MOH to contact and invite for diagnosis.

- Strictly speaking, the information to be collected through TraceTogether is limited to non-personally identifying information to reduce the risk of infringing any individual privacy.

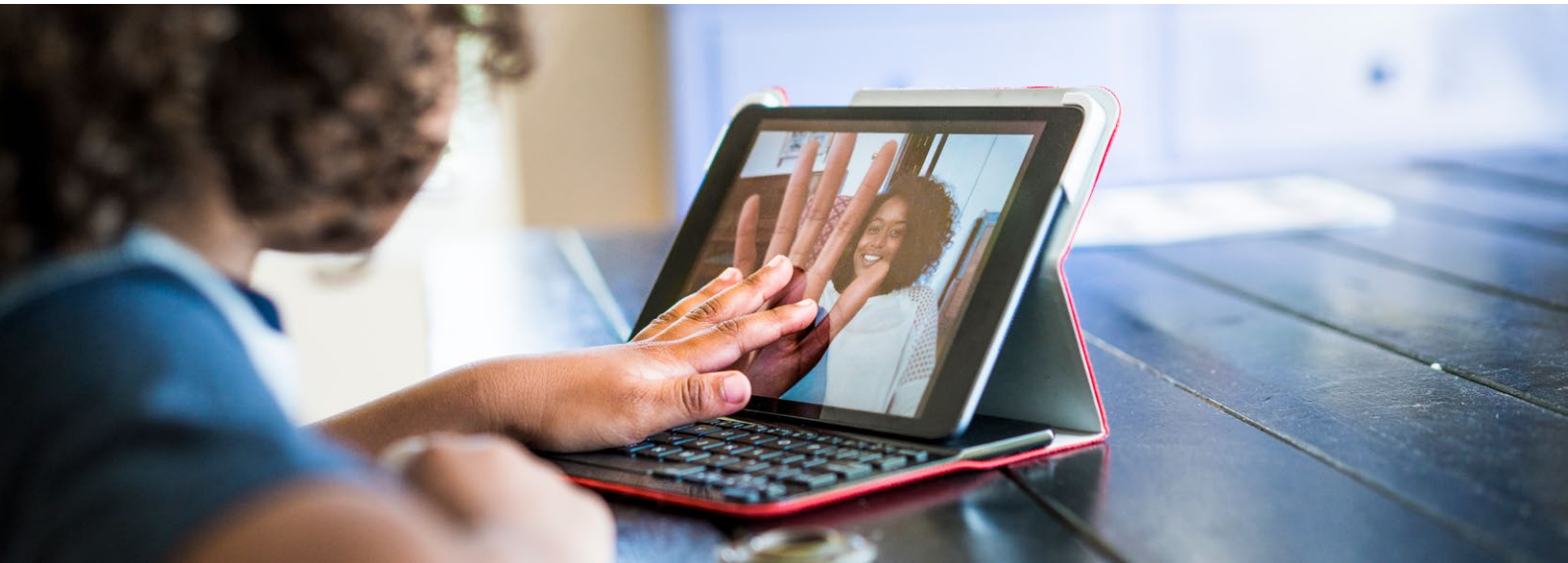
PRINCIPLE 2 – ACCOUNTABILITY

- The government in Singapore is mainly accountable for the operation of TraceTogether.

- Although laudable, this may impact its utility to public health as TraceTogether is deployed internationally. Singapore is a socially cohesive society with a high degree of trust in government. TraceTogether and other applications based on the BlueTrace protocol may struggle for the widespread adoption needed for its success in jurisdictions that do not share these characteristics. Alternatively, other jurisdictions may need to supplement the introduction of TraceTogether with mandatory rules and regulations in order to achieve the intended societal benefit. This, in turn, may create other risks or concerns, especially in relation to accountability.

- For TraceTogether, the White Paper introduces mechanisms to ensure that information would not be intercepted or Encounter Messages would not be intercepted and attacked. Encounter Information stored on individuals' devices are encrypted and TempIDs are generated randomly at intervals. However, the White Paper does not provide any solution or accountability in regards to any flaws in the solution. In particular, Project Owners have received complaints from users who had been contacted by scammers impersonating the MOH.

- Individual phone number and Encounter History, upon consent, are uploaded to the MOH's back-end server where this data is processed manually. Again, the White Paper remained silent on the counter-measures to any security breach in relation to the back-end server. No guidance was given on



how long that information will be retained in the back-end server.

- As mentioned above, one of the key elements to TraceTogether being able to succeed is the high degree of trust the people have in the local government.

- The lack of any specific legislation in Singapore which expressly provides for the protection, restricted use, security and destruction of the personal data will be seen by some as a concern. It may be that from a local perspective, some will not see this as an issue.

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- Users will be all members of the general public.

- TraceTogether does not rely on complicated technology. It is built on conventional Bluetooth technology, which has been used by smart phones for years.

- The output of the model can be explained and decisions can be audited.

- No information was disclosed in the White Paper on the provider of the Project Owner's cloud-based backend server. Similar issue was raised for the Australian COVIDSafe app where claims were made that certain US Government agencies are able to access the data covertly and certainly without notice to irrelevant individuals under the US Patriot Act and the US CLOUD Act because the Australian Government contracted with Amazon Web Services for the provision of back end server.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- There is no concern in relation to fairness & non-discrimination of TraceTogether. It is solely up to the MOH to decide how to process the information released by the consenting users. This is a matter of government policy in dealing with the pandemic instead of an issue of the Pandemic Tech Solution.

- TraceTogether will collect all Encounter Messages in the device's proximity, as long as TraceTogether is being installed.

- Concerns have been expressed that people who do not have mobile devices or mobile devises capable of downloading and operating the TraceTogether App are at a clear disadvantage. Notwithstanding the high level of mobile device proliferation in Singapore, there are some people (particularly certain senior citizens who of course are in the significant vulnerability group) who are unable to utilise the App

PRINCIPLE 5 – SAFETY & RELIABILITY

- The success of TraceTogether is significantly dependent on users providing a valid phone number upon registration and having the device with TraceTogether installed with the user at all time in order to produce reliable results. This is further restricted for users with a device that operates the iOS operating system (i.e. Apple) as BlueTooth technology does not operate in the background on iOS. This is an issue for which the Project Owner is still seeking a solution.

- The privacy safeguards will also have direct impact on the reliability of the Pandemic Tech Solution as many steps in between require manual input by users and the MOH, for example what happens if the user does not pick up the phone when being contacted by the MOH ?

- The White Paper is also silent on the effectiveness of the Pandemic Tech Solution, especially in a crowded area where BlueTooth technology may not operate as efficiently.

- The device must also be connected to the internet for at least once per day in order for the back-end server to generate sufficient numbers of TempID to be used by TraceTogether. Expert opinion suggests that, to further minimize any risk of attacks, TempID should be generated locally on individual's device.

- Data collection process is designed to render replay/ relay attack difficult, but this does not seem to be a watertight solution.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to interoperate internationally. There are mechanisms built to allow exchange of information between different

public authorities from different jurisdictions but it is unclear how this will function at the moment.

- Presently, it is not intended for the Project Owner to launch the solution in jurisdiction other than Singapore. Users from the United States and United Kingdom would be able to install and run the application provided they have a Singaporean phone number.

- The BlueTrace protocol is open sourced and the Project Owner has indicated that any other jurisdictions are free to implement locally as they deemed appropriate. This includes the COVIDSafe application launched by the Department of Health of the Australian Government.

PRINCIPLE 7 - PRIVACY

- Although this may impact the effectiveness of the Pandemic Tech Solution, the solution is designed to protect privacy data.

- Pseudonymized data (i.e. phone number) is required for the operation of TraceTogether. The Project Owner will have no other information (include the name of the owner of the phone number) even when given consent to access the data collected through TraceTogether.

- There are measurements in place to ensure that even the pseudonymized data would be difficult to be intercepted or have any value to attackers. However, it is our view that there are still areas of concerns in relation to a leakage of personal data, especially for attackers with malicious intention. Re-identification may still be possible (i.e. if the attackers managed to decrypt the TempID to retrieve the phone number of the devices and hacked the database of telecommunication companies to re-identify the user).

- Whilst the information collected does not reveal GPS or geological location, it may give rise to other valuable information such as the identity of other users that one user meets on a regular and frequent basis.

- Nevertheless, the solution is intended to fully comply with the existing privacy law. Users are able to revoke their consent at any time, and all information collected would be deleted automatically thereafter. Moreover, information will only be stored on an individual device for not more than 21 days, after which it would be automatically deleted immediately. But the White Paper is silent on the availability to users on accessing, reviewing and correcting the information stored in the device and stored with the back-end server after initial consent was given.

- Singapore has not introduced any amendments to its privacy legislation in relation to data generated by the contact tracing App. It appears that there are no plans at all for amendments to the Singapore Privacy Act. Rather, the Singapore Health Ministry's contact tracing activities and the use of collected data are already subject to sectoral rules in place under the Singaporean Infectious Diseases Act. It would also appear that collected data would be protected from misuse under the Singapore Official Secrets Act but, as mentioned, these are not specific privacy related pieces of legislation

- In contrast, privacy of data generated by the Contact Tracing App has generated significant political and social commentary in Australia. There has been a number of very prominent privacy academics and professionals who have publically stated their concerns with the privacy statements made by the Government and the privacy regulations that are being promulgated. This will have actively discouraged a number of people from downloading the App (although at the time of this key finding, there are over 5 million downloads of the App in Australia). Nonetheless, a number of high profile politicians and other people have stated that they won't be downloading the App because of privacy concerns. In response to this, the Federal Government of Australia issued a Determination (which has the effect of legislation) introducing certain privacy protections in relation to data generated by the App – including, for example, the fact that the data must be encrypted, it can only be accessed by certain personnel, it must be destroyed within a certain amount of time and so on. In addition, the Federal Government late last week issued an exposure draft of amendments to Australia's Privacy Act to give further effect to the Determination and to extend privacy protection. In other words, Australia is treating privacy protection in relation to data generated by the contact tracing App as something within the purview of Australia's privacy laws.

Nodle Coalition PostCoviData Impact Assessment ("PIA")

June 1, 2020

ItechLaw Evaluation Committee
Belén Arribas
Massimo Donna

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with Privacy Impact Assessment and whitepaper for COALITION App ("**COALITION App**").

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- COALITION App ("**COALITION App**") is designed to allow contact tracing in the general populace and proposes an architecture which is capable of international deployment.
- Coalition was conceived with an international audience in mind, therefore its creators are keen to deploy it internationally. As such the countries which take it up may have differing legal contexts and backgrounds, including in relation to general rules of law. In light of the above considerations, since Coalition may be deployed in non-democratic or quasi-democratic countries, potential deployment risk is high.
- Since Coalition may be deployed in non-democratic or quasi-democratic countries, potential deployment risk is high.
- Market/industry/sector – General use application. The app is intended to be used across all aspects of society and industry by all citizens that possess a smartphone.
- Main regulatory requirements – Data Protection (GDPR and associated legislation such as ePrivacy directive); laws applicable to the use of telecommunications networks; laws applicable to privacy, individual and mass surveillance.
- Main ethical concerns: Privacy, Right not to be discriminated against, government surveillance.
- Auditability is yet to be confirmed, but **the source code will be made open source** and publicly available for scrutiny.
- The impact of **Coalition App data processing activity is significant** – it will enable citizens who have sufficiently uptodate smartphones to understand the risk of whether they have been in contact with other infected (or potentially infected) individuals and remove them from the chain of infection by means of **notifying them to self isolate and recommending actions to mitigate against risk, including self-isolation**.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Coalition aims to provide an effective solution to fight the COVID-19 crisis, while protecting individual privacy.
- In particular, Coalition is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information with respect to other users.
- Although the system relies on the collection of information that cannot be linked to individuals (non-personal data), such information

may relate to the health of the Users, if they decide to upload their data further to testing positive.

- The Coalition App will only be downloaded and installed by Users on a voluntary basis.

- All processed data will be anonymised and Users will only notify the back-end server of their having tested positive for Covid-19 on a voluntary basis.

- These factors significantly reduce the risk of citizens' right to data protection being breached or that citizens may be discriminated against. Generally, use of the app is intended to help flatten the epidemiological curve of local Covid-19 epidemics and avoid new outbreaks by assisting with contact tracing, while protecting individual privacy.

- The solution generally complies with the ethical purposes of beneficence and non-maleficence. However, the general overarching risk of this app is that (like any other proximity/contact tracing application) it could be used for other purposes post-pandemic (i.e. for state surveillance purposes).

PRINCIPLE 2 – ACCOUNTABILITY

- The role of Nodle, from a legal standpoint, has not been clarified, hence accountability criteria are not clear.

- Major third party dependencies include:

- OS providers – Apple and Google

- BT LE System infrastructure and specification

- OS provider and BT LE infrastructure risks have already been previously identified.

- There are no third party data sources as SKs and TIDs identifiers are generated by user handsets.

- In the White Paper it states that User can, at any time, request access to the personal data that relates to User. It states further that such data are, e.g. phone number and associated random IDs. It is unclear whether a method for correcting personal data is provided

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- Users will be all members of the general public without any heightened technical sophistication.

- Data are not proprietary – they are ephemeral identifiers: ie pseudo randomised BT LE (Bluetooth Low Energy) data packets.

- The Backend and Authorisation servers should be fully auditable.

- However note that this is not a centralised system – it is highly distributed. Local data held on smartphones will be outside scope of inspection unless access is granted by (or court orders are sought effecting same).

- As the Coalition system depends on conventional BT LE technology for proximity tracing and TIDs are auto generated by phone handsets, the system should demonstrate equivalent levels of robustness which would be exhibited by any other distributed network/system.

- Coalition is susceptible to BT hacking and other cyber-risks.

- These risks are not unique to Coalition but are generic to distributed solutions of this nature.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- Although certain current aspects of the Coalition solution do not seem to be consistent with its stated characteristic of only processing anonymized personal data (i.e. during the installation process and when user self-declares positive, the app requires user's mobile phone number), the general understanding is that when deployed in a "production" environment, no personal data as defined under the GDPR will be processed. Thus, no automated individual decision making or processing as per article 22 of the GDPR will be involved in connection with the Coalition app deployment and no AI-induced discrimination appears likely.

- However, a more basic form of de facto discrimination may arise as certain segments of

the population either by reason of age, census or disability are not in a position as to own or appropriately handle smartphones or other digital devices upon which the app must be installed.

PRINCIPLE 5 – SAFETY & RELIABILITY

- Coalition, as an anonymous solution is theoretically subject to coordinated collective hacking conduct, where, for example, a number of individuals self-declare infected even if not tested positive for coronavirus with a view to sabotaging the solution. Although the likelihood of such a coordinated scheme is unlikely, should it be implemented it may cause widespread distress to people who are notified of having been close to infected individuals, even if this is not the case.

- Certain security risks have been anticipated in connection with the cryptographic technology used by the app developers, however such risks require a "tech savvy" and malicious bad actor.

- Conversely, major risks may be associated to the general population potentially attributing to the app reliability and robustness which may prove ephemeral, since they are dependent on a number of factors, including the app installation and adoption by a significant share of the populace.

- Our recommendation is that a programme of public awareness and education should be implemented in a manner befitting of the wide spectrum of public consumption.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to operate internationally.

- The solution will be made available subject to an open source license.

PRINCIPLE 7 - PRIVACY

- Whereas it might be opined that users' data are not truly anonymized, but only subjected to hard pseudonymization, it appears that only extremely tech-savvy bad actors may succeed to re-identify users' personal data.

- Therefore, it might be argued that anonymized data fall outside the field of application of the GDPR and of other data-protection legislations in the West.

Arogya Setu App ("Pandemic Tech Solution") PostCoviData Impact Assessment (“PIA”) Overarching Risk Summary (Key Findings)

May 12, 2020

by Nikhil Narendran (Trilegal, India)
Smriti Parsheera
Swati Muthukumar (Trilegal, India),
Aparajita Lath (Trilegal, India)
© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with main PIA for Arogya Setu App.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

The Pandemic Tech Solution (or **Solution**) is a mobile application developed by the Government of India with private partnership. The app developers describe it as a solution to connect essential health services with the people of India to fight against COVID-19. The Pandemic Tech Solution’s terms note that it is “*aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19*”. Further, the App's terms of use also state that the App will serve as a digital representation of an e-pass where available. The App will also provide links to convenience services offered by various service providers.The key features of the Pandemic Tech Solution include contact tracing, self-assessment by users and integration of e-pass for movement during the lockdown. The Pandemic Tech Solution uses the user's Bluetooth and GPS location data to carry out contact tracing and the underlying structure of the Pandemic Tech Solution is largely centralised. The data collected by the Solution is highly sensitive as it contains personal information including health status, location etc. albeit in a de-identified format.

The Solution may have a significant impact on the user's right to privacy, which constitutes a fundamental right. The Pandemic Tech Solution is citizen-facing. By way of notifications issued under the Disaster Management Act, 2005 (**DMA**), the Government of India has directed employers to ensure that the Solution is installed by employees on a best effort basis and empowered district authorities to advice individuals to install the Solution. While the DMA contains broad powers on measures that may be taken in response to a disaster situation, there is no specific enabling provision under the DMA which expressly permits any curtailment of the right to privacy. There are also questions as to the legal oversight of the Solution, particularly in light of the fact that India has no overarching data protection law. As per the Data Access and Knowledge Sharing Protocol, 2020 (Protocol) released by the government, the Pandemic Tech Solution may be used to make decisions in relation to sharing of a user's data for (i) directly formulating or implementing an appropriate health response, (ii) to assist in the formulation or implementation of a critical health response, or (iii) for research purposes. The Protocol also lays down other principles for the collection and processing of the data. However, the Protocol itself does not have any specific legislative basis and can be modified at any point by the Empowered Group that notified it.

Stakeholders impacted by the Solution are citizens (end users), employers, universities/research institutions or entities, government and healthcare personnel.

The Government of India along with its private partners is responsible for the Pandemic Tech Solution and departments or officers may be held responsible for certain non-compliances under the DMA. The terms of use state that the Government will make best efforts to ensure that the Solution performs as described. However, the Government will not be liable for (a) the failure of the Solution to

accurately identify persons who have tested positive to COVID-19 ; (b) the accuracy of the information provided by the Solution as to whether the persons who users have come in contact with have in fact been infected by COVID-19. This impacts the extent of responsibility and control which may be expected from the Government.

The Pandemic Tech Solution reportedly has 114 million downloads and likely a similar number of users. The data is collected constantly and it has the potential of becoming a tool of mass surveillance. The impact of processing the data is significant, as it will enable the government to understand whether Solution users have been in contact with other infected individuals and potentially remove them from the chain of infection by quarantine or isolation. It may further allow persons carrying out medical and administrative interventions necessary in relation to COVID-19 the information they might need about the user in order to be able to do their job.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The Solution has been provided by the Government of India to aid the response efforts to the COVID-19 crisis in India. Though employers and district authorities are required to ensure that the Solution is installed on a best effort basis. This could lead to a situation where employees / individuals are left with no option but to install the Solution. This may negatively impact human agency and autonomy and may have implications on a user's right to privacy and may result in loss of livelihood should they choose not to use the Solution, including by way of criminal prosecution under the DMA.

The absence of an overarching data protection law and a legislative backing to the Solution raise concerns on the legal implications and risks of harm to users. In addition to this, there is the general overarching risk of surveillance related use, false negatives, unauthorised access to data (including health data) and triangulation of user location. However, there are efforts being made to limit the period of data retention by the Solution and the manner in which data sharing can take place, which will reduce these effects to an extent.

PRINCIPLE 2 – ACCOUNTABILITY

The Solution, as initially released on 2 April 2020, was not open source and reverse engineering was also prohibited. However, the reverse engineering restriction has been removed and the Solution has been made open source at the source code level (for Android only) on 26 May 2020 i.e. nearly two months after its release. The terms of service permit users to report defects or bugs in the Solution to the Government. Given that the Solution was made open source, at the source code level, only after 26 May 2020, the App's code has not yet been audited by independent third parties. The Government has announced a bug bounty program (open till 26 June 2020) and anyone who reports vulnerabilities with the Solution will be awarded up to INR 400,000. Further, in order to ensure accountability, the Solution must also share information on the server-side code/centralization processes.

It is therefore difficult to comment on the accountability of the Solution As the Solution strives to achieve multiple purposes such as aiding both users and government authorities in responding to the COVID-19 threat, it is also difficult to determine whether the data collected is necessary and limited to such purpose.

The Solution also does not extensively apply the Privacy by Design model. This is evidenced by the fact that some users are forced to create an account and provide their data to the Solution, there is an absence of a mechanism to delete their account and the Solution collects data and stores it along with the user's personal data. While the period for retention of an individual's data by the Solution is limited and specified in its terms and the Protocol, the Solution itself does not have a defined retention term.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

There is a lack of transparency about the process of development of the Solution, including details of the private individuals and organisations that assisted the government in this initiative and the alternatives that were considered. There is also very little transparency on the Solution's use of information, accuracy of outcomes, etc. as the Solution's code (for

Android only) has only recently been made available for audit and the Government of India has not provided updates on the system architecture, data sets, processes or results. However, the Government has identified the manner in which the data collected from the Solution shall be used and the time period for which it may be retained. It is essential that the Government provides similar transparency on the Solution itself, and provides information such as the audits undergone by the Solution, the manner in which it makes decisions, etc.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The Solution does not meet accessibility standards. It is not possible to determine the quality of decisions made by the Solution at this stage due to insufficient availability of public information.

PRINCIPLE 5 – SAFETY AND RELIABILITY

The Pandemic Tech Solution has recently been made open source at the App source code level (for Android)and is largely centralised. The Solution, as initially released on 2 April 2020, was not open source and reverse engineering was also prohibited. However, the reverse engineering restriction has been removed and the Solution has been made open source at the source code level on 26 May 2020 i.e. nearly two months after its release. The terms of service permit users to report defects or bugs in the Solution to the Government. The Government has announced a bug bounty program (open till 26 June 2020) and anyone who reports vulnerabilities with the Solution will be awarded INR 400,000. Given that the Solution was made open source at the source code level only after 26 May 2020, the App's code has not yet been audited by independent third parties. Further, open sourcing has been selective and the server side source code is still not open source. There is not yet enough data on whether the Solution is functioning in the exact manner that has been specified by the government. There are news reports of ethical hackers pointing out security issues in the Solution. While these claims have been disputed by the Solution's developers, it is difficult to comment on the veracity of the claims of either side without the Solution's code being audited by multiple independent researchers.

With respect to information security certifications, the Protocol requires entities handling the Response Data to implement the ISO/IEC 27001 standard. Further, data is encrypted in transit as well as at rest. However, insufficient information is available relating to secure software development and details of implementation of encryption measures.

The privacy policy of the Solution specifies certain use restrictions. Data will be used only by the Government of India in anonymised, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualisations for the purpose of the management of COVID-19 in the country or to provide users general notifications pertaining to COVID-19 as may be required. There exists a possibility of subversion of intended use and extended state surveillance. The Government of India requires employers to ensure that employees install the Solution on a best effort basis and district authorities are also empowered to advise individuals to install the Solution. Consent will be invalid if used as part of mandatory enforcement. There is not enough data to comment on whether the Solution can be used for dual purposes.

As the Pandemic Tech Solution processes personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), any breach in security measures could violate user privacy as well as endanger the whole centralised system.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

Information on the scope of interoperability with tech solutions offered by other providers is insufficient. As per the privacy policy and Protocol for the Solution, data will be used only by the Government of India, public health institutions, Indian universities / research institution and onward transfer to third parties is restricted. Further, reuse of data for other public interest projects is also restricted as per the Protocol. Information on ownership or intellectual property rights attaching to the Pandemic Tech Solution is insufficient. At this point there isn't enough information to assess whether the Solution or data gathered by it could be distributed to other public health agencies in the world.

PRINCIPLE 7 – PRIVACY

Many of the above-described risks have adverse effects on user's privacy. The Government of India requires employers to ensure that employees install the Solution on a best effort basis and district authorities are also empowered to advise individuals to install the Solution. Consent will be invalid if used as part of mandatory enforcement. Further, children and vulnerable groups are included and there are no security safeguards for processing of the information of such groups.

While the privacy policy and the Protocol specify a data retention / deletion procedure, currently, there is no option to de-register or logout from the Solution. Since the personal data will be retained as long as the "account remains in existence", there is currently no way of ensuring that the personal data is deleted from the Solution.

There is insufficient data with respect to assessing whether beyond the data subject, the privacy of an identified group be at risk. The Solution is not very clear on what the consequences of a "yellow" or "orange" report are with respect to the self-assessment test to be undertaken on the Solution. As per the privacy policy, every time the user completes a self-assessment test, the Solution will collect their location data and upload it along with the DiD to the server. While the stated purpose is that this information will be used by the government to evaluate whether a disease cluster is developing at any geographic location, due to the lack of clarity around yellow/orange reports, it is unclear if this will be used to identify the probability of a user having COVID-19 or for any other testing-related purpose or may also expose identified group to be at risk.

There is insufficient data to show whether individuals are aware of observation at some point in time and whether and how new data is created.

CONCLUSION

The Solution has the potential of improving the predictability of the spread of COVID-19. However, since the Solution has been made open source (for Android only) at the source code level recently, there is insufficient data, as yet, on whether the Solution adheres to the highest standards of safety and reliability. However, initiative like the bug bounty program are steps in the right direction to encourage investigation of the Solution and to report vulnerabilities. Reports have highlighted significant shortcomings in terms of data security but these claims have been rebutted by the Government. Even though some of the deficiencies may have already been cured and others certainly can be rectified, there is a remainder of risks that adversely affect the fundamental human right to privacy as well as the overall reliability and efficiency of the entire Solution.

Further, as employers / district authorities may make it mandatory of individuals to install the App, the consent framework for collection of personal and sensitive personal data remains questionable. The Pandemic Tech Solution is not geared for use by people who are differently abled. Given that the Solution may be made mandatory for its use for various activities such as for right to access work place or travel, the solution is in-accessible to a large number of people. The Solution is not transparent or explainable and a person impacted with a false positive has no institutional process to challenge it. In terms of legal protections and remedies, there is no specific legal framework in place for holding the government accountable for privacy breaches except general constitutional remedies that flow from the recognition of privacy as a fundamental right.

Estimote, Inc. Workplace Safety Wearable Overarching Risk Summary (Key Findings)

May 12, 2020

by Jenna F. Karadbil (Law Office of Jenna F. Karadbil, P.C., New York, NY, United States) with contributions by Doron Goldstein (Katten Muchin Rosenman LLP, New York, NY, United States) and Dean W. Harvey (Perkins Coie LLP, Dallas, TX, United States)

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with the PIA for Estimote's Workplace Safety Wearable, dated May 15, 2020. There is very little public information available on the Estimote wearable solution, so this review has been based on the available documentation, the CEO's interview and third party documentation, both cited in the PIA.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

In early April 2020, Estimote, Inc. launched its workplace safety wearable device solution to assist companies with contact tracing and identification of infected or exposed employees. Estimote is a for-profit company based in Krakow, Poland that was formed in or around 2012. The solution aims to help companies save money by maintaining a safe workplace and quickly identifying and resolving risks. The solution is a modification of an existing "panic button" wearable, which, when deployed with other Estimote beacon technology, is used by employees to alert management to an event, with the Estimote beacons identifying where in the company building the employee is experiencing such event. The new workplace safety wearable is virtually the same hardware, with new code snippets created to add in the contact tracing and health identification services.

The goal of the Estimote solution is to identify infected or symptomatic employees (by virtue of their pressing a button on the wearable) and accelerate and focus containment measures by the company both for exposed employees and in the identified areas of the company. The solution is fully dependent on the infected or symptomatic employee reporting their positive COVID-19 diagnosis or experiencing of symptoms. The backend of the solution cannot serve its actual function without obtaining such information from the infected employee's wearable device. The solution is not currently customer or publicly focus, and is instead intended to be used solely within a company's physical locations.

The Estimote solution stores information, presumably employee names, locations, durations in locations, contacts with other employees, and healthy status. No specifics of the solution have been released ; thus it is unknown what information is stored on the wearable, transmitted from the wearable via cellular network to the backend, and is maintained on the backend. There is no information as to how long all of this sensitive information is stored, how it is stored, where it is stored, who has access to it, whether it can be exported or shared, and whether Estimote will have access to or host any of the implementing companies' data or systems.

Because the Estimote solution is meant to be used by companies world-wide, it is possible that several countries' laws and regulations would apply both to Estimote and the implementing companies. As such, there is an inherent risk for employees where the solution is deployed in countries that do not have strong (or any) data protection laws and regulations, workplace monitoring and safety laws and regulations, laws against discrimination, telecommunications regulations, collective bargaining agreements, regulations for wearable devices, regulations for medical devices, and protections from mass surveillance.

The main ethical concerns are that (a) mandatory usage and sharing of employee health data, (b) employee privacy, (c) transparency about who can see and use the data, (d) security of the data, and (e) what else it might or could be used for outside of the intended purposes. These concerns are further compounded by the fact that each company that implements the solution is responsible for its

own implementation, unless Estimote assists in operating it or providing its hosted cloud services for the backend of the solution.

Though the individuals directly affected by data processing are limited to users of the wearable device, voluntarily providing their data to their company, the solution could have an impact on the general public by helping implementing companies quickly identify and contain possible outbreaks. The Estimote solution was developed and deployed very quickly upon the COVID-19 crisis becoming a worldwide pandemic. It has been deployed in several companies, though no usage or deployment data has been released by either Estimote or any of the implementing companies.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The Estimote solution is being deployed to protect employees from other employees by enforcing social distancing guidelines, alerting companies to employees that fail to comply with social distancing guidelines, and to help quickly identify potential exposures and attempt to contain further exposures in the workplace. The Estimote solution aims to assist companies, not the general public, though, as noted above, the implementation of the solution by companies could have a positive impact on the general public by helping to identify and contain possible outbreaks. Further societal benefits could include helping employees come back to the workplace from being furloughed or in an unpaid status, help employees and their family members feel safe both in their workplace and at home knowing they have not been exposed at work, helping companies maintain clean workplaces and products both for employees and customers, and if tests are limited, help identify those employees that should be tested based on their exposure(s).

There is minimal autonomy provided to the employee in that they have the option to not wear the device, to turn it off or to let it die and not replenish the charge. In practice, however, there may not be any actual autonomy, as employee's work or job retention may be based on mandatory usage. Importantly, the entire solution may not work effectively if employees choose to opt-out of wearing the device, as it would not be able to effectively contact trace potentially exposed employees or locations. While employee data is said to be anonymized either on the device or in the transmission from the device to the backend, the Estimote dashboard makes de-anonymization appear very easy. Employees also would appear not to have any control (or potentially even knowledge) of how, where, when, and by whom, their personal data is de-anonymized and shared.

Although Estimote intends for the wearing of the device to be voluntary, doing so may adversely affect the solution's efficacy. Thus, there is a conflict betweeen employee autonomy and effectiveness of the solution.

Successful attacks on the information security or widespread malicious use of the device and its data have the potential to weaken the acceptance of and trust in the solution to contain the pandemic at the workplace. If the solution is easily hackable or manipulated, does not work as intended, or is used for uses not consented to, then it could affect both Estimote's and the implementing companies' reputation and business.

The use of a centralized system increases the risks of attacks and that data collected through the device and on the backend could be used for unintended purposes, including nefarious purposes, such as surveillance and location tracking outside the workplace.

Because each company will have its own implementation of the Estimote solution, it is possible that other legal, cross border, policy, or contractual obligations could apply that have not been mentioned or reviewed in this PIA.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, the Estimote solution is largely dependent on third-party company implementations since the solution is fully programmable by the implementing companies. Estimote has not disclosed what portions are not customizable. These risks are unknown, as company implementations appear to be private, and should arguably at least stay somewhat private, to help protect their employees' sensitive information.

This appears to be Estimote's first foray into a device aimed specifically at a health crisis, though the originating panic button device could be used to notify of a health-related event or emergency. It is unknown how or whether there will be any support provided for the solution, including if employees have issues with the devices or companies have issues with the backend or customization.

Importantly, Estimote has not updated its Privacy Policy since 2015, including not making any adjustments after the enactment of GDPR, including in its home country, Poland. The Privacy Policy does not mention or appear to apply to the wearable solution.

The principles of necessity, proportionality and data minimization have not been disclosed. No privacy measures have been disclosed, other than the fact that data will be transmitted in anonymized form to the backend, and viewable in the backend in anonymized form until the company wishes to de-anonymize it. The company could potentially use and share the de-anonymized data for both intended and unintended purposes.

Development and deployment are funded by Estimote, a private company. Therefore, if it turned out that mitigating some of the risks identified in this PIA would come with additional costs, it unknown whether Estimote would decide to spend more rather than accept both avoidable and unacceptable risks. Though, not doing so could have an impact on its reputation and business.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

While there is transparency in use of the device, as an employee can clearly see who is wearing one, there is very little transparency with respect to everything else about the solution. Further, an employee should assume that at least some of his or her personally identifying information is stored and processed by the back end, as that would be inherent in any properly working contact tracing solution.

It is unknown how or what personally identifying information of the employees is contained in the solution, and employees appear to generally not have access to any of their data stored or used by the solution. However, each implementation will be based on the specific implementing company's existing data and requirements.

There are no specific Terms of Service for the Estimote solution. Estimote's existing Terms of Service are from 2015 and do not mention or appear to cover wearables. While Estimote's undated Terms of Sale appear to apply to other Estimote goods, they do not specifically mention the wearable solution, nor do they mention the predecessor it was based on – the panic button solution.

It is unknown what terms will apply for employees that use the device, as the company that implements the wearable will likely be entering into the agreement with Estimote, not any individual employees. Thus, employees could then be subject potentially to Estimote's terms, but also any terms and/or policies of their employer.

While the general solution is fairly explainable, it does not include specifics as to the wearable or backend, or to any company's implementation.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

In terms of accessibility, the device should be able to be used by any and all persons, as it is wearable either on a neck lanyard, wrist device, or as an access card. Since the wearer does nothing but turn it on, it should be usable by anyone, including those with limited capacity or ability.

The quality of the data is subject to the veracity of the employees using it as well as the potential accuracy limitations of Bluetooth and LTE technology. Thus, there could be reporting of false positives and corrective action taken, when, in fact, it was not actually necessary. Or, failures to report in order to maintain one's job or paycheck, which could expose other employees and sites within the company. So, there is a risk that employees will purposely not report, though less of a risk that employees will falsely report, their infected statuses.

The quality of the data is also subject to proper functioning of the wearable, transmission means and the backend. If the device malfunctions and a report is not registered or transmitted to the backend, then employees would be left open to potential exposure and great health risk.

Because companies can collect location data, not just for purposes of contact tracing, its usage could be unfair and/or used in a discriminatory manner.

PRINCIPLE 5 – SAFETY AND RELIABILITY

Very little technical data has been released, so no technical analysis of the Estimote solution has been performed, including assessing the security and reliability of the solution. This is very concerning, as employees are likely to expect their person and sensitive data to be both secure and accurate. The wearable is relatively new, with the prior device having been released just a few years ago. No reliability or security data has been released on the original device, or this new workplace safety version.

Employees are at risk of their data being disclosed and potentially used for unintended purposes. An employee's infected status could be made public without their authorization. Or, an employee could be tracked outside of the company or during non-working hours to create a full picture of each of the employee's movements.

The backend contains all of the data from the wearables, plus additional identifying data about the employees. A breach of the centralized server could lead to revealing all of the data and personal information contained in the solution. Each implementing company will be responsible for securing their own environment, unless they utilize Estimote's cloud hosted environment, in which case Estimote should have primary responsibility. It is unclear whether Estimote will have access to a company's data, in addition to the implementing companies. It is also unclear whether the data will be shared with any third parties, as the Privacy Policy is so old that it does not cover this wearable solution. It is possible that the device could also transmit data back to Estimote, or elsewhere, not just to the company that has implemented the solution.

Although unlikely, the device could be considered a medical device and then would be subject to medical device regulations. Particularly, if the company customizes the implementation to be assisted in its function by pharmacological, immunological or metabolic means. However, the EU has extended the time period for compliance with its medical device regulations until next May.

Although Estimote has noted that the data is securely transmitted from the device to the backend, no information as to how this is accomplished has been disclosed.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The Estimote solution is proprietary and owned by Estimote, including all intellectual property, as no parts of it appear to be open sourced. Currently the solution will be used solely by Estimote's company customers, though public health uses are being explored. Companies will likely enter into some form of a license agreement with Estimote for the use of the wearable and the backend. Users may then be subject to their employer's policies or agreement with respect to their use of the wearable.

As noted above, it is unknown whether Estimote will have access to the data collected by the device

or processed on the backend, in addition to the implementing company. The device is not meant to do anything other than its intended purpose, however, it is fully programmable and thus can be altered to serve other purposes.

PRINCIPLE 7 – PRIVACY

No specific information has been provided as to what data is stored on the devices or on the backend, though based on the limited disclosures, certain data can.

be inferred to be collected. Based on images and description on Estimote's website, it appears that an employee's movements, proximity (and duration) to other employees, and actual (or believed) infection is collected and stored by the backend. The movement and proximity data is likely to be stored by the device before being transmitted to the backend. It is known whether the employee's personal information is stored on the device, or in the backend, or both. It also appears that specific location within the company can be collected if used in conjunction with out Estimote beacon technology, or via the limited indoor GPS capabilities of the device.

While Estimote believes that employees should opt-in, there is no stated method for obtaining consent. The Estimote Terms of Service state that the company is responsible for obtaining the necessary rights from the employee, but there are no specifics as to the scope of consent required. Further, as noted above, the Terms of Service are from 2015 and do not address wearable devices, nor GDPR requirements.

Under the GDPR, data subjects have the right to access information being processed about him or her and may request correction or deletion of their data under certain circumstances, however, there is no information disclosed about how this will work either with Estimote or the implementing companies. Estimote appears to view itself as acting as a processor, though the language of its documentation make that less than fully clear. Estimote appears to be relying on its customers (the implementing companies) to have determined the lawful basis for processing, and states in its Privacy Policy that "Customer Data Is owned and controlled by our customers...we collect and process Customer Data solely on behalf of our customers...." There do not appear to be any requirements on control of data.

There is no information available regarding security processes, de-identification, or anonymization of the information to be collected and stored by the implementing companies, nor by Estimote.

CONCLUSION

The Estimote solutions presents several high risks largely due to the lack of information and disclosures about the solution. While employees may benefit from a solution that helps them stay safe and healthy, it is unknown whether the Estimote solution will, in fact, do so. There is no information on the majority of the principles set forth in the PIA. This includes information as to the serious privacy, cybersecurity and related concerns that the technology raises, as well as analysis of the potential legal and regulatory requirements, such as those under privacy and data protection laws and regulations (i.e., GDPR, CCPA, PIPEDA), workplace monitoring and safety laws and regulations, laws against discrimination, telecommunications regulations, collective bargaining agreements, regulations for wearable devices, regulations for medical devices, and protections from mass surveillance.

The centralized solution presents a weak point which is further exacerbated by the apparently lack of standards on implementations. While some implementing companies may have rigorous security, need to know disclosures, and opt-in participation, there will likely also be companies that don't. If the central server is compromised, the entire system would then likely be compromised, including employee health and location data. However, in order for the solution to be effective, employees should opt-in, yet doing so gives up virtually all of their autonomy and control over their own data.

Lastly, the reliability of the solution is also unknown. If the devices malfunction, it could put employees and potentially the company's customers at risk.

TerraHub
Credential Link PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

May 26, 2020

by Adrien Basdevant, Caroline Leroy-Blanvillain (Basdevant Avocats, France)

© ItechLaw Association 2020, CC-BY-SA

To be read in conjunction with main PIA for TerraHub Credential Link Solution, dated 26 May 2020.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

TerraHub has developed a verification platform for workers, products, and processes. The company's product, Credential Link builds an irrefutable audit trail for worker training, authorizations, and health self-assessments. It thus provides workforce management tools for verifying and sharing health self-assessments, safety and professional certificates. In the early days of COVID-19, TerraHub recognized that its Credential Link solution might have a role in controlling the spread of the virus. On this platform, employers have access to critical worker information before they arrive on site. Accordingly, employees are now able to upload for example COVID-19 test results or training courses relating to sanitary measures.

Each individual has the following data associated with them: personal identity information, credential details, credential verification details, audit trail history, employer and project associated details. The total volume of data for each individual is under 500Kb (average). However, aggregate data for analytics is spread across an entire organization's user base. So, organizations can have a relatively large amount of data to work with to make decisions based on analytic data.

Three stakeholders were identified: the organization deploying the tool (i.e the employer), the workers using the tool (i.e the employees) and the organizations issuing the credentials (i.e the issuers). The Solution works with the Hyperledger Fabric blockchain protocol. Each individual is authenticated using a public key that is registered when the individual is given access to the relevant shared private channel. The data cannot be read nor updated by any individual not previously registered. There are two kind of access: user access and admin access. Admin access is limited to authorized roles from the employer. Specific symptoms reported by the worker can only be accessed by that worker. Employer gets an OK/Not OK summary for each worker without any detailed elements relating to the self-assessment. Data may be shared with the third parties by giving explicit consent and access can be revoked by the worker. Third parties are the organizations to which the worker gives the authorization to access the data.

This update of the solution has been released in April 2020 to help companies ensure the safety of employees returning to work after the lockdown period. The main ethical concerns may relate to the following points:

- Whether the blockchain-based technology used allows the users to effectively exercise their rights (re modification / erasure) ;
- Whether both the technology used, and the algorithm added for the health self-assessment are transparent and explainable ;
- Whether the use of Credential Link by the employer might affect the rights and interests of employees, for example by creating discriminatory situations ;
- Whether the governance of the solution clearly frames the secondary use of data inferred from the solution by the employer.

A supplemental PIA is useful in the context of the implementation of the Pandemic Tech Solution to exit the sanitary crisis and help secure workplaces. Indeed, the relationship between employer and

employees is deemed to be unbalanced per se, and accordingly it should be assessed whether the use of this Solution by the employer may threaten the rights and interests of the employee.

More specifically, three ethical concerns have been identified at this point:

- How to ethically frame the decisions taken by the employer when receiving a "NOT OK" summary from the Solution ?
  - For example, might a "NOT OK" worker obliged to stay home suffer from a salary loss or a red flag in its relating personnel file ?
  - Also, what would happen in a given organization, if an employee refuses to use this solution ?
  - How does the "OK/NOT OK" summary is completed ? Can we infer information from this summary ?
- How to ensure that the employee will not overpass or lie on the self-assessment to avoid any repressive action from the employer ?
  - For example, might an employee afraid of repressive action lie on the self-assessment health status and thus render the Solution inefficient by putting at risk other workers of the company ?
  - NB: The irrefutable nature of a blockchain technology is useful if and only if the primary source of information is reliable.
- Are there any ways to use this data by the employers for different purposes initially planned ?
  - Is the data provided by the employee stored on-chain or off-chain ?
  - Is there a way for employer to store a copy of this data ? (e.g screen shots)

Additionally, the Solution collects and displays to the employer sensitive data, for which it must be ensure maintaining security and integrity as well as preserving a certain control from the employees.

This PIA should help both TerraHub and Project Owner to deploy the Solution with respect to legal and ethical principles to trade-off between organization's interests of workplace safety and rights and privacy of workers.

It should be noted that part of the assessment leading to the issue of the OK/NOT OK summary is based on a simple algorithm (i.e. for the health self-assessment) that is not deemed to integrate AI or machine-learning as defined in the present Pandemic Impact Assessment framework. However, such completion should be considered if complementary information about the functioning of the algorithm could indicate otherwise.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The solution is currently deployed in Canada only, but might completely be deployed in other regions/ countries which could significantly modify the risk rating relating to the legal framework. The relevance and proportionality of the use of Credential Link should be assessed by the Project Owner with regard to the excessive surveillance of employees that it may engender.

Furthermore, while deploying this solution, it should particularly be assessed who will be subject to the use of the solution (i.e. only employees or any person entering a site of the Project Owner) and how the data will be use to limit any infringement to the rights of users.

High risks were also identified regarding the use of the Summary by the employer, which might significantly affect the autonomy of workers and thus should be carefully framed. The Project Owner should consider not to take decisions significantly affecting the autonomy and / or dignity of workers on the sole basis of the solution at stake.

Finally, considering that information about credentials and self-assessments is stored off-chain, it partially prevents the data from being publicly available in an irrevocable manner. Accordingly, it remains the responsibility of each issuer to implement appropriate safeguards including time-limit or automatic deletion of the information. However, it should be noted that the worker can revoke the authorizations granted to access the data, which appears as a minimum appropriate safeguard as well.

PRINCIPLE 2 – ACCOUNTABILITY

Centralized and decentralized components should be detailed, regarding both the protocol and/or the governance of the solution. Accordingly, the governance of Credential Link should be determined precisely by the Project Owner, as it is the first step to rate the level of risk inherent to the implementation of the solution. Some measures were taken by TerraHub to limit the technical and privacy risks, nonetheless it will also depend on the way the organization will deploy and implement Credential Link.

Also, sufficient measures should be implemented to determine if the decision-making process allows Project Owner operators to adjust parameters, to follow or not the Summary output, etc.

Data is stored both on and off chain. Off chain data require encryption and a distributed model uses QLDB ; off chain data requires encryption stored in S3. On chain, are only stored the hashes that point to all the off-chain sources so as to ensure no changes are made off-chain. All "issuers" are identified by the network as the originators of a credential. Employer can define an administrator that can access public employee information, for example credentials, but not health self-assessments. An employer can be an "issuer" and a "reader", and they can define an administrator that can access public employee information, for example credentials, but not health self-assessments.

The Project Owner should ensure at all time it remains accountable for the responsible deployment of the Solution, including by means of “human-in-the-loop” or “human-over-the-loop” to make sure that humans oversight is active and involved in relation to recommendation provided by the “OK/NOT OK” Summary.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

Two issues must be distinguished when assessing transparency and explainability criteria for Credential Link: the permissioned blockchain protocol, on the one hand, and the private algorithmic decision making tool, on the other hand. Indeed, regarding the health self-assessment, an algorithm is implemented in the solution to assess whether a worker presents risks of exposure to COVID-19. This algorithm consists in a basic survey on the employee’s latest actions deemed to be “at-risk” (e.g. traveling, symptoms, contact with infected person). Considering that no access was given to the survey nor the algorithm itself, it is not possible to determine the risk rating of obtaining a false summary. Nor it is possible to determine if the outputs of the algorithms could be explained or if the functioning of the algorithm could be explained (black-box situation). It is assumed that the use of such a basic algorithm contributes to limiting this risk but does not eliminate it completely as false positives or false negatives are still possible, thus questioning the transparency of the application. As far as the blockchain protocol is concerned, in

order to limit the risks regarding explainability, the Project Owner should take appropriate measure to make sure that such innovative and complex technology is being fully understood by its users.

Moreover, it seems that very few materials are currently available to users, which may identify a mitigation measure to be taken. The functioning of the solution should be explained to employees, with all the consequences attached to the use of that solution. No opacity should remain on the conditions of use, the privacy issues, and how the solution works.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The data processed by Credential Link is only modified but not transformed, or only to the extent of providing the Project Owner with the summary but in that case, only the granularity of available data changes.

Besides, inequalities inherent to the use of the application may arise between workers familiar with technologies and the ones for whom the use of blockchain technology means very little. More precisely, if the use of Credential Link is not mandatory but voluntary or incentive, it should be assessed whether all workers will be able to acknowledge all the outputs of accepting to use it. This can relate to the idea of an "ethically" free and informed consent. Indeed, such a consent to use the app may be guided by employer pressure, or social pressure, for example if there are beneficence or maleficence effects attached to the use of Credential Link, which could appear infringing the fairness principle.

Finally, the risk of having derivative misuse of the application appears high if no conditions are clearly set while implementing it.

PRINCIPLE 5 – SAFETY AND RELIABILITY

It appears that TerraHub implemented strong technical and organizational measures to ensure both safety and confidentiality of the Pandemic Tech Solution, by adopting recognized technical standards including encryption all along the transactions. The most pregnant risk remaining relates to the redress mechanisms, for example in case of hacking resulting in the loss of the credentials, as no information has been provided on that point.

The blockchain technology used lowers the risk of falsification, once the hash of the data is stored on-chain, but could not guarantee that the original source of the data stored off-chain is reliable.

However, the risk of dual use is assumed to be high, as once the Project Owner has the lead on the solution and collect inferred data, it becomes difficult to control any subversion of intended use.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The fact that Credential Link relies on an open source blockchain protocol increases transparency and prevent from most of infringement risks to intellectual property rights.

More generally, when assessing such a solution working with a blockchain protocol and a algorithm layer, this Principle should be assessed with regards to each part of the solution, as the analysis may vary considering the blockchain protocol (here open-source) or the algorithm (here proprietary and non-public).

PRINCIPLE 7 – PRIVACY

There is often a warning to be issued when employer / employee relationship is at the core of the use of a technology. In the present case, there might be risks regarding the preservation of workers' privacy, which TerraHub has tried to limit at best to only grant access to the minimum information required. The employee keeps control over the provided data, both with the authorization system and the possibility to disactivate the application.

Nevertheless, risks remain regarding the use by the employer / Project Owner of the information extracted from Credential Link. The major concern with this solution was about the information being stored on-chain, which would have resulted in the impossibility to exercize the rights of correction and/or erasure thus severely affecting the rights of workers. It appears that workers' data is stored off-chain and is accordingly not publicly available, and consequently the retention period and deletion

of the data remain of the sole responsibility of the organizations storing it.

It should also be noted that regarding specifically the answers to the health self-assessment, the worker cannot modify them anymore once submitted, but can re-take the survey. The Project Owner should assess whether appropriate safeguards are implemented regarding the rights to privacy of workers, notably by determining efficient processes for employees to exercise their rights.

If Privacy and Data Protection concerns remain reasonable regarding the design of Credential Link, further risks appear when considering secondary use of the data by Project Owner. More specifically, it is here considered the possibility for Project Owner to process any derived or inferred data collected from the summary or any other feature provided by the solution. Such a use could entail severe consequences for the workers and should be consciously framed when deploying Credential Link within an organization.

CONCLUSION

The Credential Link solution seems to offer some safeguards to reach its purpose: ensuring a safe return to work for organizations adopting it. However, two kinds of risks should be particularly observed: i) risks inherent to the design of the solution itself, and ii) risks linked to the implementation of the solution by the Project Owner.

Regarding the risks inherent to the solution itself, the present Pandemic Impact Assessment reveals that the worker data is at least stored off-chain, which limits the risk of rending the data constantly and publicly available on the blockchain. The fact that data is stored off-chain results in the transfer of responsibility to the organization by which the data is stored for implementing appropriate retention period and erasure processes, with respect to the principle of data minimization that could lead the choice of adopting a Pandemic Tech Solution. Besides, the Project Owner should in either way ensure that any organization accessing the worker's data, or processing derived or inferred data, implemented adequate retention periods and processes for workers to effectively exercise their rights, thus making sure for the end-user that all the information will eventually be deleted from systems of third parties to which s.he granted authorization at once. It should also be highlighted that the use of blockchain, if it allows to have irrefutable and accurate data, also entails the impossibility to verify the veracity of the updated data

Furthermore, regarding the specific question of the summary made available to the employer, it should be noted that the health self-assessment is based on a simple algorithm: it determines if a worker is OK by tallying the answers and indicating OK if the person has no symptoms, has not travelled or come into contact with a sick person. Once the answers are submitted, the worker cannot modify the answers, but can take the survey again. Therefore, it should be assessed the possibility for the employer to access the previous results of the assessment or whether only the latest results are displayed which could contain a risk of falsification if the worker takes the test again to artificially modify the result. However, the possibility for the employer to access the previous results would potentially infringe the principles of necessity, proportionality, and data minimization. Consequently, arises a trade-off between privacy preservation and workers' protection on the one hand, and the need for accuracy on the other hand.

Another identified risk is the lack of documentation available for the end-user. Due to the context in which the assessment was led, maybe this documentation has just not come to our attention, but it seems that no Terms of Use or Privacy Policy is available for the solution. Terms of Use appear to be of crucial importance, as the use of Credential Link by employers may have significant consequence on employees in case of misuse (both by the employee in case of lie and by the employer in case of disrespectful secondary use).

CONCLUSION (SUITE)

Regarding the risks inherent to the adoption of the solution by the Project Owner, more significant concerns should be raised. First, the consequences of the summary sent to the employer should be precisely determined and discussed prior to the adoption of the solution, to prevent any infringement to the rights of employer and any discriminatory measures. For example, if the daily summary indicates that the worker is “NOT OK” (i.e. s.he cannot access the workplace without putting at risk its coworkers), there should be a procedure indicating if the worker shall stay home, but it should also be documented what it implies concretely. More precisely, it could be imagined that if the worker is in incapacity of accessing safely the workplace because s.he does not hold verified COVID-19 testing results, it will entail a loss of salary corresponding to the time spent home, which might be deemed as a discriminatory measure as if the solution had not been implemented, the employee would not have suffered such a loss.

The other major risk in the context of implementation of the solution relates to the secondary use of the data made by the Project Owner. While considering adopting a Pandemic Tech Solution as Credential Link, it should be assessed to what extent analytics or secondary use of the collected data may be done. This point partially relates to the previous one as secondary use should be determined to avoid any use against the employee and making sure there will be no misusage leading to discriminatory situation, whether by comparing the data from a particular worker to another or by using the data to make decision that would not benefit the workers and that would not have been taken without access to this data.

Mitigation measures should integrate a specific internal body ensuring to respect the rights of workers while thinking of the implementation of Credential Link.


Bitte halten
Sie Abstand!

BIBLIOGRAPHIE

RAPPORT, DÉCLARATIONS

1. Atlantic Council, *COVID-19's potential impact on global technology and data innovation*, avr. 13, 2020. https://atlanticcouncil.org/blogs/geotech-cues/COVID-19s-potential-impact-on-global-technology-and-data-innovation/ (consulté le mai 13, 2020).
2. Académie des Sciences, *COVID-19 pour une surveillance basée sur le volontariat*, https://www.academie-sciences.fr/pdf/rapport/2020_04_10_avis_tracage.pdf (Consulté le mai 13, 2020
3. J. Bay, "Automated contact tracing is not a coronavirus panacea", *Government Digital Service - Singapore*, https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 (consulté le mai 13, 2020).
4. Comité Consultatif National d'Ethique, *La contribution du CCNE à la lutte contre COVID-19 : Enjeux éthiques face à une pandémie*, https://www.ccne-ethique.fr/fr/publications/la-contribution-du-ccne-la-lutte-contre-COVID-19-enjeux-ethiques-face-une-pandemie (consulté le mai 13, 2020).
5. Comité national pilote d'éthique du numérique, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, https://www.ccne-ethique.fr/sites/default/files/publications/bulletin-1-ethique-du-numerique-covid19-2020-04-07.pdf, (Consulté le mai 13, 2020)
6. Commission de l'éthique en science et en technologie, "Enjeux éthiques liés à la pandémie de COVID-19", https://www.ethique.gouv.qc.ca/fr/publications/ethique-covid19/ (consulté le mai 13, 2020).
7. Council of Europe, *Modernisation of the Data Protection "Convention 108"*. https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet (consulté le mai 31, 2020).
8. Council of Europe, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (consulté le mai 31, 2020).
9. Council of Europe, Committee of Ministers, *Algorithms and automation: new guidelines to prevent human rights breaches*, https://www.coe.int/en/web/cm/news/-/asset_publisher/hwwluK1RCEJo/content/algorithms-and-automation-new-guidelines-to-prevent-human-rights-breaches/16695 (consulté le mai 31, 2020).
10. Datenschutz, *Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie*. https://www.datenschutzkonferenz-online.de/media/en/Entschlie%C3%9Fung%20Pandemie%2003_04_2020_final.pdf, (consulté le 31 mai 2020)
11. *Déclaration de Montréal pour un développement responsable de l'IA*, https://www.declarationmontreal-iaresponsable.com (consulté le mai 13, 2020).
12. European Commission, *Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, (consulté le 31 mai 2020)
13. European Commission, "Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures", *Shaping Europe's digital future*, avr. 16, 2020. https://ec.europa.eu/digital-single-market/en/news/coronavirus-eu-approach-efficient-contact-tracing-apps-support-gradual-lifting-confinement (consulté le mai 31, 2020)
14. European Data Protection Board, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandCOVID-19_en.pdf, (consulté le mai 31, 2020)
15. European Data Protection Supervisor, *Monitoring spread of COVID-19*, https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_COVID-19_monitoring_of_spread_en.pdf, (consulté le mai 31, 2020)
16. Fédération internationale des Droits de l'Homme, "Covid 19 - Prioriser les droits humains et protéger les plus vulnérables", https://www.fidh.org/fr/regions/afrique/COVID-19-prioriser-les-droits-humains-et-proteger-les-plus (consulté le mai 13, 2020).
17. Future of privacy Forum, *Artificial Intelligence and the COVID-19 Pandemic*, https://fpf.org/2020/05/07/artificial-intelligence-and-the-COVID-19-pandemic/ (consulté le mai 13, 2020).
18. "G20 Trade and Digital Economy Ministers adopt statement in Tsukuba", *Trade - European Commission*. https://trade.ec.europa.eu/doclib/press/index.cfm?id=2027 (consulté le mai 31, 2020).
19. Information Commissioner's Office, *Data protection impact assessments*, avr. 15, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (consulté le mai 31, 2020).
20. Information Commissioner's Office, *Sample DPIA template*, https://iapp.org/media/pdf/resource_center/dpia-template-v04-post-comms-review-20180308.pdf, (consulté le mai 31, 2020)
21. ITechLaw, *Responsible AI: A Global Policy Framework*, juin 14, 2019. https://www.itechlaw.org/ResponsibleAI (consulté le mai 31, 2020)
22. M., Mahjoubi , N*ote parlementaire Version 1.0 du lundi 6 avril 20*, http://d.mounirmahjoubi.fr/TracageDonneesMobilesCovidV1.pdf, (consulté le mai 13, 2020)
23. McKinsey, *Contact tracing for COVID-19: New considerations for its practical application*, https://www.mckinsey.com/industries/public-sector/our-insights/contact-tracing-for-COVID-19-new-considerations-for-its-practical-application?cid=other-eml-alt-mip-mck&hlkid=828ba682899043c9b4626cffc6748619&hctky=2723747&hdpid=c8873e56-2263-4a01-b712-ccf574693275 (consulté le mai 13, 2020).
24. A. Olbrechts, "Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19", *Comité Européen de la Protection des Données - European Data Protection Board*, avr. 22, 2020. https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_fr (consulté le mai 13, 2020).
25. *PEPP-PT Pan European Privacy Protecting Proximity Tracing,* https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf, (consulté le mai 31, 2020)
26. Personal Data Protection Commission - Singapore, *Model artificial intelligence governance framework*, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf, (consulté le mai 31, 2020)
27. US Federal Trade Commission, *Using Artificial Intelligence and Algorithms*, avr. 08, 2020. https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms (consulté le mai 31, 2020).
28. World Economic Forum, *Gig workers among the hardest hit by coronavirus pandemic*, https://www.weforum.org/agenda/2020/04/gig-workers-hardest-hit-coronavirus-pandemic/ (consulté le mai 25, 2020).

RÉFÉRENCES ACADÉMIQUES

29. Ada Lovelace Institute, *COVID-19 Rapid Evidence Review: Exit through the App Store?*, https://www.adalovelaceinstitute.org/our-work/COVID-19/COVID-19-exit-through-the-app-store/ (consulté le mai 13, 2020).
30. C. Batut et A. Garnero, "L'impact du COVID-19 sur le monde du travail : télémigration, rélocalisation, environnement", *Le Grand Continent*, https://legrandcontinent.eu/fr/2020/05/01/limpact-du-COVID-19-sur-le-monde-du-travail-telemigration-relocalisation-environnement/, (consulté le mai 31, 2020)
31. A. Casilli, *En attendant les robots*. Le Seuil, 2019.
32. X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay, C. Vuillot, *Le traçage anonyme, dangereux oxymore. Analyse de risques à destination des non-spécialistes*, https://risques-tracage.fr/docs/risques-tracage.pdf, (consulté le mai 13, 2020)
33. M. Foucault, Surveiller et punir. *Naissance de la prison*. Editions Gallimard, 2014.
34. Le Centre de recherche en éthique, *Les enjeux éthiques des applications anti-pandémie*, http://www.lecre.umontreal.ca/les-enjeux-ethiques-des-applications-anti-pandemie/ (consulté le mai 13, 2020).
35. E. Lemonne, "Ethics Guidelines for Trustworthy AI", FUTURIUM - *European Commission*, déc. 17, 2018. https://ec.europa.eu/futurium/en/ai-alliance-consultation (consulté le mai 31, 2020).
36. Leopoldina, Nationale Akademie der Wissenschaften, *Coronavirus-Pandemie – Die Krise nachhaltig überwinden*, https://www.leopoldina.org/publikationen/detailansicht/publication/coronavirus-pandemie-die-krise-nachhaltig-ueberwinden-13-april-2020/ (consulté le mai 31, 2020).
37. D. Rotman, "COVID-19 has blown apart the myth of Silicon Valley innovation", *MIT Technology Review*, https://www.technologyreview.com/2020/04/25/1000563/COVID-19-has-killed-the-myth-of-silicon-valley-innovation/ (consulté le mai 13, 2020).
38. B. Sportisse, "Contact tracing", *Inria*, https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux (consulté le mai 13, 2020).
39. J. Stanley, J. S.Granick, "The Limits of Location Tracking in an Epidemic", *American Civil Liberties Union*, https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf, (consulté le mai 13, 2020)

PRESSE, MÉDIAS

40. "Individual vs Group Privacy", *IThappens.nu*, mars 20, 2019. http://www.ithappens.nu/individual-vs-group-privacy/ (consulté le mai 31, 2020).
41. J. Dingel et B. Neiman, "How many jobs can be done at home?", *VoxEU.org*, avr. 07, 2020. https://voxeu.org/article/how-many-jobs-can-be-done-home (consulté le mai 25, 2020).
42. D. Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero*, https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 (consulté le mai 13, 2020).
43. H. Guillaud, "StopCovid : le double risque de la "signose" et du "glissement"", *Medium*, https://medium.com/@hubertguillaud/stopcovid-le-double-risque-de-la-signose-et-du-glissement-b1e2205bff5a (consulté le mai 13, 2020).
44. A. Marty, "Ce que L'automatisation visuelle apportera au monde Post-COVID-19", *Forbes France*, mai 04, 2020. https://www.forbes.fr/technologie/ce-que-lautomatisation-visuelle-apportera-au-monde-post-COVID-19/ (consulté le mai 25, 2020).
45. E. Massé, "Privacy and public health: the dos and don'ts for COVID-19 contact tracing apps", *Access Now*, https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-COVID-19-contact-tracing-apps/ (consulté le mai 13, 2020)
46. E. Morin, "Nous devons vivre avec l'incertitude", *CNRS Le journal*. https://lejournal.cnrs.fr/articles/edgar-morin-nous-devons-vivre-avec-lincertitude (consulté le mai 13, 2020).
47. F. Saadi, "COVID-19 et retail : un nouveau fonctionnement s'impose pour les distributeurs", *L'Usine Digitale*, https://www.usine-digitale.fr/article/COVID-19-et-retail-un-nouveau-fonctionnement-s-impose-pour-les-distributeurs.N961681 (consulté le mai 25, 2020)

LISTE DES CONTRIBUTEURS

COMITÉ DE PILOTAGE

Jean-Louis Davet
Président
Denos Health Management
Paris

David Doat
Maître de conférences en philosophie
Université catholique de Lille (Laboratoire ETHICS)
Lille

Marie Élaine Farley
Présidente – Chef de la Direction
Chambre de la Sécurité Financière
Montréal

Anne-Marie Hubert
EY, Associée directrice
Institut de la technologie pour l'humain, Présidente
Montréal

Nathalie de Marcellis-Warin
CIRANO, Présidente – Directrice
Polytechnique Montréal / OBVIA, Générale Professeure titulaire
Montréal

Charles S. Morgan
International Law Association, Président
McCarthy Tétrault LLP, Associé
Montréal

Eric Salobir
Président
Human Technology Foundation
Paris

PROJECT LEAD

Adrien Basdevant
Avocat fondateur
Basdevant Avocats
Paris

Caroline Leroy-Blanvillain
Avocat
Basdevant Avocats
Paris

INSTITUT DE LA TECHNOLOGIE POUR L'HUMAIN

ANALYSTE

Pierre Gueydier
Directeur de la recherche
Human Technology Foundation
Paris

COMMUNICATION

Antoine Glauzy
Directeur
Institut de la technologie pour l'humain
Montréal

Sibylle Tard
Responsable du Lab.222
Human Technology Foundation
Paris

ÉQUIPE ÉTHIQUE

Allison Marchildon
Professeure agrégée
Université de Sherbrooke / OBVIA
Montréal

Manuel Morales
Professeur agrégé
Université de Montréal / Fin-ML Network / OBVIA
Montréal

Yves Poullet
Université de Namur / Université Catholique de Lille (ETHICS)
Recteur honoraire de l'Université de Namur, professeur associé à l'Université Catholique de Lille
Namur

Bryn Williams-Jones
Professeur titulaire
Ecole de Santé Publique de l'Université de Montréal / OBVIA
Montréal

EQUIPE JURIDIQUE (ASSOCIATION ITECHLAW)

Belén Arribas Sanchez
Partner
Andersen Tax & Legal
Barcelone

Edoardo Bardelli
Trainee lawyer
Gattai, Minoli, Agostinelli & Partners
Milan

John Buyers
Partner
Osborne Clarke LLP
Londres

Philip Catania
Partner
Corrs Chambers Westgarth
Melbourne

Ellen Chen
Associate
McCarthy Tétrault LLP
Montréal

Massimo Donna
Managing Partner
Paradigma Law
Milan

Licia Garotti
Partner
Gattai, Minoli, Agostinelli & Partners
Milan

Marco Galli
Avvocato
Gattai, Minoli, Agostinelli & Partners
Milan

Doron S. Goldstein
Partner
Katten Muchin Rosenman LLP
New York City

Dean W. Harvey
Partner
Perkins Coie LLP
Dallas

Lara Herborg Olafsdottir
Partner
Lex Law Offices
Reykjavik

Charles-Alexandre Jobin
Associate
McCarthy Tétrault LLP
Montréal

Jenna F. Karadbil
Founder
Law Office of Jenna F. Karadbil, P.C
New York City

Rheia Khalaf
Director
University of Montreal
Collaborative Research & Partnerships *Fin-ML/IVADO*
Montréal

Aparajita Lath
Associate
Trilegal
Bangalore

Kit Mun Lee
Associate
Corrs Chambers Westgarth
Melbourne

Swati Muthukumar
Associate
Trilegal
Bangalore

Nikhil Narendran
Partner
Trilegal
Bangalore

Smriti Parsheera
Fellow
CyberBRICS Project
New Delhi

Patricia Shaw
CEO
Beyond Reach Consulting Limited
Londres

Alexander Tribess
Rechtsanwalt Partner
Weitnauer Partnerschaft mbB
Hambourg

Padraig Liam Walsh
Partner
Tanner De Witt Solicitors
Hong Kong

Alan Wong
Registered foreign lawyer – Solicitor
Tanner De Witt Solicitors
Hong Kong

EQUIPE TECHNIQUE

Victor de Castro
Chief Medical Officer
Philips Health Systems
Paris

Maxime Fudym
Developer
Waxym
Paris

Roberto Mauro
Managing Director Europe, Strategy & Innovation Center
Samsung Electronics

Gilles Mazars
Director of Engineering – Advanced Innovation Lab
Samsung Electronics
Paris

Pascal Voitot
Samsung Electronics
Applied Research Scientist in Deep/Machine Learning – Advanced Innovation Lab
Paris

Jean-Jacques Wacksman
Developer
Waxym
Paris

MERCI À NOS PARTENAIRES


Sector 2
Sector 3